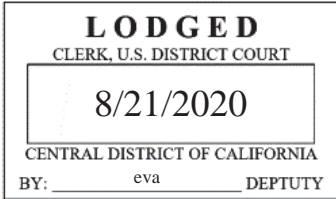


AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

Original Duplicate Original



UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America

v.

AHMED BINYAMIN ALASIRI,
aka Kevin Lamar James,

Defendant.

Case No. 8:20-mj-00554-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

On or about the dates of July 24, 2020 and August 6, 2020, in the county of Orange in the Central District of California, the defendant violated:

Code Section

21 U.S.C. §§ 841; 846

Offense Description

Distribution of Methamphetamine and
Conspiracy to Distribute
Methamphetamine

This criminal complaint is based on these facts:

Please see attached affidavit.

Continued on the attached sheet.

/s/ COLIN M. DWYER

Complainant's signature

Colin M. Dwyer, Special Agent, FBI

Printed name and title

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

Date: August 21, 2020

City and state: Santa Ana, California



Hon. JOHN D. EARLY, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Colin M. Dwyer, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since March 2012. Since May 2018, I have been assigned to the Los Angeles Field Office, Orange County Resident Agency and a member of the FBI's Joint Terrorism Task Force ("JTTF"), which is comprised of law enforcement agents and officers from federal, state, and local agencies, assigned to investigate international terrorism. Prior to my assignment on the JTTF, from August 2016 to May 2018, I served on the Drug Enforcement Administration's ("DEA") Southern California Drug Task Force, High Intensity Drug Trafficking Area and investigated large-scale drug trafficking organizations. I received approximately 20 weeks of formal training at the FBI Academy in Quantico, Virginia. I also completed the DEA Task Force Officer School, where I received an additional 20 hours of instruction in investigative matters related to drug trafficking. While in law enforcement, I have assisted in numerous investigations involving the unlawful importation, transportation, and distribution of controlled substances, including but not limited to cocaine, crack cocaine, heroin, methamphetamine, and marijuana. During these

investigations, I have conducted physical surveillance, monitored subjects, and executed search and arrest warrants.

2. This affidavit is made in support of a criminal complaint and arrest warrant for Ahmed Binyamin Alasiri ("ALASIRI"), also known as Kevin Lamar James, for violations of Title 21, United States Code, Sections 841 (Distribution of Methamphetamine) and 846 (Conspiracy to Distribute Methamphetamine).

3. This affidavit is also made in support of search warrants for: (1) the person of ALASIRI ("ALASIRI'S PERSON"); (2) ALASIRI'S residence, located at 9852 Gamble Avenue, Garden Grove, California 92841 (the "SUBJECT PREMISES"); and (3) ALASIRI'S vehicle (the "SUBJECT VEHICLE"). ALASIRI'S PERSON, the SUBJECT PREMISES, and the SUBJECT VEHICLE are further described in Attachment A-1, A-2, and A-3, respectively. The requested search warrant seeks authorization to search the person and locations, as described in Attachment A-1 through A-3, for the items to be seized described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841 (Distribution of Methamphetamine) and 846 (Conspiracy to Distribute Methamphetamine) (the "Subject Offenses").

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

warrants 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 and all dates and times are approximate.

II. SUMMARY OF PROBABLE CAUSE

5. As detailed below, in July and August of 2020, ALASIRI sold methamphetamine, and a substance represented as Methylenedioxymethamphetamine ("MDMA"), also known as "Ecstasy", to an FBI undercover employee ("UCE") in a series of drug buys at the SUBJECT PREMISES.¹

6. On July 11, 2020, ALASIRI, without prompting, advised the UCE that he operated a drug trafficking business and offered to sell the UCE various controlled substances. In the same conversation, ALASIRI quoted a price of \$3,300 for the UCE to purchase a pound of methamphetamine. On three occasions in July and August 2020, ALASIRI sold controlled substances to the UCE. On July 23, 2020, ALASIRI sold 10 multi-colored pills believed to be MDMA to the UCE for \$100. The following day, ALASIRI sold the UCE approximately one pound of methamphetamine for \$3,700. Laboratory tests confirmed that the substance ALASIRI sold was Methamphetamine Hydrochloride, approximately 96 percent pure, for a total of approximately 430 grams of actual methamphetamine. On August 6, 2020, ALASIRI sold approximately

¹ The suspected MDMA remains at the DEA Southwest Laboratory pending testing.

one pound of methamphetamine to the UCE for \$3,700. Preliminary laboratory analysis identified the substance as Methamphetamine Hydrochloride, approximately 98 percent pure, for a total of approximately 435.12 grams of actual methamphetamine. Following the August 6th transaction, ALASIRI agreed that he was willing to continue to sell the UCE methamphetamine.

III. STATEMENT OF PROBABLE CAUSE

A. ALASIRI is Convicted of Terrorism, Serves a Lengthy Custodial Sentence, and is Released in Garden Grove, California

7. According to publicly available court records, on December 14, 2007, ALASIRI, then known as Kevin Lamar James,² pleaded guilty to one count of violating Title 18, United States Code Section 2384 (Conspiracy to Levy War Against the United States Government through Terrorism). United States v. James, 05-CR-00214-CJC, Docket Number ("Dkt. No.") 262. Specifically, ALASIRI admitted to conspiring with others to engage in violence against the governments of the United States and Israel by attacking targets in Southern California associated with the U.S. military and the Jewish religion. Id. On March 9, 2009, United States District Judge Cormac J. Carney sentenced ALASIRI to 192 months imprisonment and three years of supervised release. Dkt. No. 368.

² On November 7, 2019, Kevin Lamar James filed a Decree Changing Name petition with the Superior Court of California, County of Orange, Central Justice Center to change his name to Ahmed Binyamin Alasiri. The Court ordered the completion of his name change on that same date.

8. According to U.S. Bureau of Prisons ("BOP") records, ALASIRI served the last five years of his custodial sentence at the U.S. Penitentiary, Administrative Maximum (ADX), in Florence, Colorado. In May 2019, ALASIRI was released to a halfway house in Garden Grove, California. Following his release from the halfway house, ALASIRI began serving his three-year supervised release term.

B. Undercover Investigation

9. The following information is based on my review of investigative reports, audio and video recordings, and screen-captures of communications between ALASIRI and the UCE.

10. On June 4, 2020, ALASIRI met with the UCE in person, and began sharing living space with the UCE. After the meeting, ALASIRI and the UCE communicated via telephone calls, text messages, social media, and in person.

11. According to records provided by T-Mobile and the UCE's observations of ALASIRI's mobile phone, to communicate with the UCE and others ALASIRI used an Apple iPhone 7 ("ALASIRI's iPhone"), bearing IMEI 354913094571433, registered to telephone number 323-910-9794, and subscribed in ALASIRI's name.

1. ALASIRI Sells MDMA and Methamphetamine to the UCE

12. According to audio and video recordings I reviewed, on July 11, 2020, ALASIRI and the UCE traveled to Los Angeles

together in the SUBJECT VEHICLE. The SUBJECT VEHICLE is a four-door 2007 Mercury Mariner Hybrid sports utility vehicle bearing vehicle identification number 4M2CU39H87KJ07043 and California License Plate 5XNF130, and registered to "Ahmed B. Alasiri."

13. While driving, the topic of selling drugs to the UCE was raised for the first time. ALASIRI spontaneously commented to the UCE that "they have a lot of meth addicts" (presumably referring to the area through which they were driving) and pointed out "people selling right there." ALASIRI then described various family members' criminal activity and named a cousin as a well-known drug trafficker. ALASIRI elaborated on the cousin's possession of "weed," how much he (ALASIRI) charges his own customers for "weed," and stated that "I know weed because I'm around it." ALASIRI stated, "I have another cousin that presses the "X pills," and that he (ALASIRI) sold "pills" and "weed" to various persons. ALASIRI also told the UCE about specific customer requests, stating, "What he wanted was some powder and crystal." ALASIRI then said, "I have connections to every single drug you can imagine." ALASIRI told the UCE that, from his "crystal source," "I can give you thirty-three hundred a pound." ALASIRI also told the UCE, "at a hundred dollars I give you a hundred pills". ALASIRI and the UCE then discussed "ice," "the brown," "China white," and "the black." ALASIRI stated, "I got edibles, too." ALASIRI then handed to the UCE packages of "edibles" from within the SUBJECT VEHICLE. The UCE had not discussed purchasing drugs from ALASIRI prior to this car ride.

a. Based on my knowledge, training, and experience investigating drug trafficking offenses and my conversations with the UCE, I know that the words ALASIRI used in this conversation to describe the drugs to which he has "connections" are slang terms for marijuana ("weed"), marijuana-laced foods ("edibles"), MDMA also known as Ecstasy ("X pills" and "pills"), cocaine ("powder"), methamphetamine ("crystal," referred to by the UCE as "ice"), and various forms of heroin and opioids ("the brown," "the black," and "China white"). Further, I understand that in this conversation ALASIRI offered to sell the UCE methamphetamine (referring to it as "crystal"; also referred to by the UCE as "ice") at three thousand three hundred dollars per pound ("I can give you thirty-three hundred a pound"), and one hundred MDMA pills ("X pills" and "pills") for one hundred dollars ("At a hundred dollars I give you a hundred pills").

14. On July 15, 2020, the UCE and ALASIRI, using ALASIRI's iPhone, engaged in a text message conversation I have reviewed, in which the UCE asked if ALASIRI could sell him, in coded language, methamphetamine and MDMA. In this conversation, the UCE wrote:

Also I talked to some people who interested in the food your cousin be cooking. They wanted a sample so I'll probably grab like 20 to let them try it. And probably a pound from your boy you told me about that cook the meat too.

ALASIRI responded by text message, "Okay."

a. Based on my knowledge, training, and experience investigating drug trafficking offenses and my conversations

with the UCE, I believe the UCE was arranging to buy controlled substances ("the food") and that the UCE requested ALASIRI provide "a sample" of twenty pills of MDMA ("20"), and one pound of methamphetamine ("the meat").

15. On July 23, 2020, the UCE met with ALASIRI at the SUBJECT PREMISES, where they share living space, to buy the controlled substances discussed in the prior text messages. The UCE recorded their conversation, and I have reviewed the recording. During this meeting, ALASIRI asked the UCE, "What are you trying to get?" The UCE responded, "A pound of the ice . . . if you can." ALASIRI responded "A pound of ice? That's crystal, right?" The UCE confirmed, "Yeah, yeah." The UCE and ALASIRI then discussed the price of a pound of methamphetamine. ALASIRI asked the UCE, "Are you getting any of the pills?" ALASIRI told the UCE that he did not know how much to charge the UCE for the pills because a street dealer usually sells them for him. The UCE stated, "Give me 10, I'mma give you a hundred." ALASIRI then provided the UCE with ten multi-colored pills believed to be MDMA, in exchange for \$100. The UCE and ALASIRI returned to discussion of the methamphetamine price. The UCE gave ALASIRI \$3,500 for one pound of methamphetamine, to be delivered to the UCE at a later time, and left the SUBJECT PREMISES.

16. Immediately after leaving the SUBJECT PREMISES with the ten multi-colored pills believed to be MDMA, the UCE gave me the pills, which were transported and processed directly into FBI evidence.

17. Later that evening, the UCE again met with ALASIRI at the SUBJECT PREMISES. The next day, again at the SUBJECT PREMISES, the UCE gave ALASIRI an additional \$200 for the methamphetamine purchase.

18. On July 24, 2020, surveillance units observed ALASIRI driving the SUBJECT VEHICLE to multiple locations throughout Los Angeles and meeting with various persons. At one point, ALASIRI was seen leaving a residential area with a small package wrapped in plastic in his hand and getting into the SUBJECT VEHICLE. After making more stops, ALASIRI drove the SUBJECT VEHICLE back to the SUBJECT PREMISES. FBI surveillance observed ALASIRI leave the SUBJECT VEHICLE carrying various bags and a package and go into the SUBJECT PREMISES.

19. The UCE met ALASIRI upon his return to the SUBJECT PREMISES. According to the video recording of the interaction I reviewed, ALASIRI gave the UCE a plastic bag containing an off-white crystalline substance packaged inside of a white Styrofoam container. ALASIRI then stated, "That's very strong stuff, from what I hear" and "I can get anything whenever you need." ALASIRI later continued "That's . . . that's a, that's a easy gig right there," and agreed he would sell the UCE more methamphetamine in the future.

20. After retrieving the package from ALASIRI at the SUBJECT PREMISES, the UCE provided me the plastic bag containing an off-white crystalline substance packaged inside of a white Styrofoam container, immediately after leaving the SUBJECT

PREMISES. The package was then transported and processed directly into FBI evidence.

2. Testing Confirms the Substance ALASIRI Sold the UCE was Methamphetamine

21. The DEA Southwest Laboratory in Vista, California analyzed the crystalline substance ALASIRI sold the UCE and issued a Chemical Analysis Report that identified the crystalline substance as Methamphetamine Hydrochloride, with an approximate net weight of 448 grams, substance purity of approximately 96 percent, and a pure substance weight of approximately 430 grams.

3. ALASIRI Again Sells Methamphetamine to the UCE

22. On August 6, 2020, the UCE met with ALASIRI at the SUBJECT PREMISES and provided ALASIRI \$3,700 in cash. The UCE audio/video recorded their meeting, and I have reviewed that recording. ALASIRI and the UCE then briefly discussed pricing schemes for future controlled substances transactions and the UCE left the SUBJECT PREMISES. Later that evening, the UCE returned to the SUBJECT PREMISES. While there, ALASIRI led the UCE to the plastic bag containing an off-white crystalline substance packaged inside of a white Styrofoam container. ALASIRI then agreed to continue selling methamphetamine to the UCE. The UCE left the SUBJECT PREMISES and immediately provided me the package he received from ALASIRI, which was then transported and processed directly into FBI evidence.

4. Testing Confirms the Substance ALASIRI sold the UCE was Methamphetamine

23. The DEA Southwest Laboratory in Vista, California conducted preliminary testing of the plastic bag containing an off-white crystalline substance packaged that ALASIRI provided the UCE. According to a preliminary testing report provided to me via email on August 19, 2020, the laboratory determined the off-white crystalline substance was Methamphetamine Hydrochloride, with an approximate net weight of 444 grams, substance purity of approximately 98 percent, and a pure substance weight of 435.12 grams.

C. Probable Cause that Evidence of the Subject Offenses will be Found on ALASIRI'S PERSON, at the SUBJECT PREMISES, and in the SUBJECT VEHICLE

24. ALASIRI'S PERSON: ALASIRI personally sold controlled substances to the UCE. UCE recordings show ALASIRI in possession of controlled substances. The UCE saw ALASIRI using and in possession of a device believed to be an iPhone.

25. SUBJECT PREMISES: The UCE gave ALASIRI the money to buy methamphetamine at the SUBJECT PREMISES, and ALASIRI returned to the SUBJECT PREMISES with the methamphetamine. ALASIRI possessed purported MDMA pills at the SUBJECT PREMISES and sold them to the UCE at the SUBJECT PREMISES. The UCE observed ALASIRI using a device believed to be an iPhone at the SUBJECT PREMISES.

26. SUBJECT VEHICLE: Surveillance teams report that ALASIRI primarily drives the SUBJECT VEHICLE. ALASIRI was seen driving the SUBJECT VEHICLE to transport the methamphetamine the UCE purchased on at least one occasion. ALASIRI also possessed the marijuana-laced foods in the SUBJECT VEHICLE. The UCE observed ALASIRI using a device believed to be an iPhone while ALASIRI was driving the SUBJECT VEHICLE.

IV. TRAINING AND EXPERIENCE REGARDING DRUG OFFENSES

27. From my training, personal experience, and the collective experiences related to me by other trained investigators with experience in drug trafficking investigations, I am aware of the following:

a. Drug trafficking is an ongoing or continuing criminal activity that occurs over months and often years, and drug traffickers, or those that assist in that venture, maintain and tend to retain accounts or records of those transactions. Drug traffickers tend to keep these accounts and records in their residence(s), vehicles safes, storage containers, and in other areas under their control.

b. Because drug traffickers frequently continue their criminal activity indefinitely, they keep records of their illegal activities for a period of time extending beyond the time during which they actually possess controlled substances, in order to maintain contact with criminal associates for future drug transactions, and to have records of prior transactions for

which, for example, they might still be owed controlled substances proceeds, or might owe someone else money. Because possession of the documents themselves, unlike possession of controlled substances, is not illegal, drug traffickers often fail to take precautions to destroy or conceal the documentation. Therefore, documentation may survive for many months, sometimes years, after a large volume of drug transactions have occurred, often in the traffickers' residences and vehicles.

c. Drug traffickers often maintain books, records, receipts, notes, ledgers, bank records, money orders, and other papers relating to the cultivation/manufacture, transportation, ordering, sale and distribution of illegal controlled substances. These individuals commonly "front" (provide on consignment) illegal controlled substances to their clients and, thus, keep some type of records or communication concerning monies owed. The aforementioned books, records, communications, receipts, notes, ledgers, etc., are maintained where the drug trafficker has ready access to them, that is, in places that include the drug traffickers' respective residence(s), place(s) of business, vehicles, as well as locations from which the drug trafficker conducts drug transactions.

d. Drug traffickers often place their assets in names other than their own to avoid detection of those assets by law enforcement; those persons are commonly family members, spouses or companions, friends, and associates who accept titles of assets to help the trafficker avoid discovery and detection.

e. Individuals involved in drug trafficking often conceal evidence of their illegal activities, including drugs, drug proceeds, and packing materials in their residences, or the residences of friends or relatives, and in surrounding areas to which they have ready access such as garages, carports, storage areas, and outbuildings. They also conceal evidence in vehicles, including vehicles outside of their residences, so that they can hide it from law enforcement, including law enforcement officers executing search warrants at their residences or businesses.

f. Drug traffickers generally sell drugs for cash proceeds. Drug traffickers often have on-hand large amounts of United States currency in order to maintain and finance their ongoing business. Drug traffickers often keep large sums of currency, caches of drugs, financial instruments, precious metals, jewelry, automobiles, and other items of value and/or proceeds of drug transactions, including evidence of financial transactions related to obtaining, transferring, secreting, or spending large sums of money acquired from engaging in the acquisition and distribution of controlled substances in their residence, vehicles, safes, storage containers, and in other areas under their control. Unexplained wealth is probative evidence of crimes motivated by greed, in particular, drug trafficking.

g. When drug traffickers amass large quantities of cash from the sale of drugs, they will sometimes attempt to legitimize these profits through the use of banks and financial

institutions and their services, including account, securities, traveler's checks, cashiers' checks, money order, wire transfers, certificates of deposit, and safe deposit boxes. Records from such transactions are often maintained in residences, offices, garages, storage buildings, automobiles, and safe deposit boxes.

h. Drug traffickers and distributors commonly use vehicles to further their distribution operations, such as using vehicles to meet with controlled substances buyers, to transport controlled substances to and from stash locations, to conduct controlled substances and cash exchanges, and to transport proceeds from controlled substances transaction locations to stash locations and/or banks.

i. Drug traffickers often conceal, in various locations of their vehicles, including non-manufacturer hidden compartments, which they have ready access to, cash, drugs, drug paraphernalia, automobile titles, deeds to property, and other items of value and/or proceeds of drug transaction, as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money acquired from engaging in drug trafficking activities.

j. Furthermore, drug traffickers often alter the manufactured voids of vehicles to hide and conceal drugs and drug proceeds. Drug traffickers also often remove the insulation from manufactured voids within the vehicle, including door panels, to create additional space to hide and conceal drugs and drug proceeds.

k. Drug traffickers use telephones, portable cellular and digital telephones, pagers and other communication devices, sometimes in fictitious and/or other individuals' names, and maintain telephone and address books, telephone bills and other books and papers that reflect names, addresses, and/or telephone numbers of their associates in the drug trafficking organization and customers of controlled substances. These digital devices are often stored in their vehicles.

l. Drug traffickers often carry multiple mobile phones, in addition to their personally used mobile phone, in order to remain in contact with the owners of the drugs, to compartmentalize their communications, and for other purposes related to drug trafficking as described in detail above.

m. Drug traffickers and distributors commonly use debit calling cards and wireless communications technology (such as paging devices and cellular phones - including smartphones with electronic mail capability - and computers), and often maintain within their cellular phones and other digital devices telephone numbers and addresses of their drug trafficking associates, as well as other evidence of their illegal activity, such as photographs, text messages, web site information, electronic records of transactions or amounts paid and owed, and travel records.

n. Drug traffickers and distributors, who deal with large quantities of controlled substances and money, commonly use firearms when conducting controlled substances transactions to protect their controlled substances supplies and/or proceeds.

Drug traffickers and distributors often keep their firearms close at hand, including in their vehicles.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES³

28. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

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

³ 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.

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.

29. 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:

i. 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.

ii. 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.

30. 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.

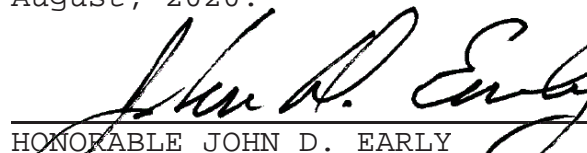
31. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress ALASIRI's thumb and/or fingers on the device; and (2) hold the device in front of ALASIRI's face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

VI. CONCLUSION

32. For all the reasons described above, there is probable cause to believe that ALASIRI violated Title 21, United States Code, Sections 841 (Distribution of Methamphetamine) and 846 (Conspiracy to Distribute Methamphetamine). In addition, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found on ALASIRI's PERSON, at the SUBJECT PREMISES, and in the SUBJECT VEHICLE, as described in Attachments A-1, A-2, and A-3.

/s/ COLIN M. DWYER
Colin M. Dwyer, Special Agent
Federal Bureau of
Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 21st day of August, 2020.


HONORABLE JOHN D. EARLY
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A-1

PERSON TO BE SEARCHED

The person of Ahmed Binyamin ALASIRI, also known as Kevin Lamar James, 44 years old, approximately 6'1" tall and approximately 185 pounds, with black hair and brown eyes, depicted below:



The search of ALASIRI shall include any items on his person or within his immediate vicinity and control capable of containing items to be seized, including clothing pockets, containers such as briefcases, backpacks, boxes, and any digital devices.

ATTACHMENT A-2

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is the residential property located at 9852 Gamble Avenue, Garden Grove, California 92841. The SUBJECT PREMISES is a tan, one-story residential house with a pitched roof, located on the south corner of Gamble Avenue and Aldgate Avenue. There is a garage attached to the house, and a large driveway in front of the residence. The address of the residence is clearly marked above the garage and is visible from Gamble Avenue. There is no fence around the front of the property; however, there is a wall along the southwest and southeast sides of the property, separating the SUBJECT PREMISES from immediately neighboring residences.



ATTACHMENT A-3

PROPERTY TO BE SEARCHED

The SUBJECT VEHICLE is a four-door 2007 Mercury Mariner Hybrid sports utility vehicle, bearing vehicle identification number 4M2CU39H87KJ07043 and California License Plate 5XNF130, and registered to "Ahmed B. Alasiri."



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841 (Distribution of Methamphetamine) and 846 (Conspiracy to Distribute Methamphetamine) (the "Subject Offenses"), namely:

a. Any controlled substance, including MDMA or methamphetamine in any form, paraphernalia associated with the use, storage, distribution, possession and/or manufacture of controlled substances, including but not limited to scales, drug packaging materials, containers associated with the storage of controlled substances, various other chemicals, utensils, equipment or apparatus associated with the manufacture of controlled substances, books, articles and commercially printed matter relating to the use, distribution, possession and/or manufacture of controlled substances;

b. Books, records, notes, ledgers, and other papers relating to the transportation, ordering, purchase, and distribution of controlled substances. These records may exist in the form of paper documents or as information stored within a computer, cell phone, or another electronic device;

c. Address books, and any other papers reflecting names, addresses, and/or telephone numbers;

d. Indicia of occupancy, residency and/or ownership of the premises described above, including, but not limited to

utilities and telephone bills, cancelled envelopes, keys and lease agreements, loan records and/or any other document which contains indicia of occupancy;

e. Automobile titles, deeds to property, and other items of value and/or proceeds of drug transactions, as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money;

f. U.S. currency and any other financial instruments or proceeds;

g. Firearms, ammunition, or other dangerous weapons;

h. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, including the Apple iPhone 7 bearing IMEI 354913094571433, and forensic copies thereof.

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

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

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

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

v. evidence of the times the device was used;

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

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

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

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

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

3. 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.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

4. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications:

Non-Digital Evidence

5. Prior to reading any document or other piece of evidence ("document") in its entirety, law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search (the "Search Team") will conduct a limited review of the document in order to determine whether or not the document appears to contain or

refer to communications between members of the Federal Public Defender's Office (to include Nadine Hettle and Gary Rowe) and any person ("potentially privileged information"). If a Search Team member determines that a document appears to contain potentially privileged information, the Search Team member will not continue to review the document and will immediately notify a member of the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case). The Search Team will not further review any document that appears to contain potentially privileged information until after the Privilege Review Team has completed its review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to the Search Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed

together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Search Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

8. The Search Team will search for digital devices capable of being used to facilitate the subject offenses or capable of containing data falling within the scope of the items to be seized. The Privilege Review Team will then review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and

transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like: Federal Public Defender's Office, Nadine Hettle, Gary Rowe, or their email addresses, and generic words such as "privileged", "work product", and "attorney-client". The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this

review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

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

15. If either the Privilege Review Team or 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, they shall immediately discontinue the 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.

16. 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.

17. 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.

18. 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 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.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, 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.

20. 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.

21. In order to search for data capable of being read or interpreted by a digital device, the Search Team is 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, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. During the execution of this search warrant, with respect to any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of the person 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 the face of the person 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.

23. 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.