SEALED

AO 91 (Rev. 11/11) Criminal Complaint

FILED

MAY 21 2019

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY _____ DEPUTY CLERK

UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

OMAR ISHO

Defendant(s)

Case No. 2:19-MJ-0081-CKD

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 February 9, 2019 to May 15, 2019 in the county of Sacramento and San Joaquin in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Distribution of a Controlled Substance

This criminal complaint is based on these facts:

See Affidavit of U.S. Postal Inspector Andrew Cornwell, attached hereto and incorporated by reference.

☑ Continued on the attached sheet.

Complainant's signature

U.S. Postal Inspector Andrew Cornwell
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/21/2019

Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

PENALTY SLIP

United States v. Omar Isho

COUNT ONE:	21 U.S.C. § 841(a)(1) – Distribution of a Controlled Substance Fine of up to $1,000,000, and/or Imprisonment of up to 20 years, or both Mandatory 3 years supervised release
COURT ASSESSMENT:	$100

AFFIDAVIT OF US POSTAL INSPECTOR ANDREW CORNWELL

I, Andrew Cornwell, being first duly sworn, hereby depose and state as follows:

I. AGENT BACKGROUND

1. I am a United States Postal Inspector assigned to the San Francisco Division of the United States Postal Inspection Service (USPIS), and have been so employed for two years and eight months. I am currently assigned to the USPIS Narcotics Enforcement and Criminal Investigations (NECI) Task Force in Stockton, California. The NECI Task Force investigates postal related crimes including the theft of the United States Mail, and the related crimes of identity theft, check fraud, credit card fraud, narcotics and narcotics proceeds being trafficked through the mail. I was previously employed as a Police Officer with the Arlington, Texas Police Department for nine years and six months. My last three years at the department were spent as a Detective with the APD Robbery/Gang Investigations Unit and the Economic Crimes Unit. The Robbery/Gang Investigations Unit investigated all robberies and any gang related violent crime or organized crime in the city. The Economic Crimes Unit investigated all fraud and computer related crimes occurring in the city.

2. I have received training and investigated cases involving financial crimes, thefts, computer and communications-related crimes, organized drug crimes, identify theft, money laundering and narcotics. I have undergone twelve weeks of Postal Inspector Basic Training in Potomac, Maryland. This training involved the investigation of mail theft, identify theft, drug trafficking and fraud. Through my training, experience, and interaction with other experienced Postal Inspectors, Task Force Officers, and other drug trafficking investigators, I have become familiar with the methods employed by drug traffickers to smuggle, safeguard, store, transport, and distribute drugs; to collect and conceal drug-related proceeds; communicate with other participants to accomplish such objectives, and the manner in which drug traffickers use the mail to conduct their illegal operations.

3. During my training, experience, and interaction with other experienced Postal

Inspectors, Task Force Officers, and other drug-trafficking investigators, I have become familiar with the methods employed by drug traffickers to smuggle, safeguard, store, transport, and distribute drugs; to collect and conceal drug-related proceeds; and to communicate with other participants to accomplish such objectives. I have received specialized training and instruction in narcotics investigation matters including, drug interdiction, drug detection, money laundering techniques and schemes, and drug identification.

II. PURPOSE

4. This Affidavit seeks to establish probable cause to believe that **OMAR ISHO** has, within the Eastern District of California, engaged in conduct that constitutes a violation of 21 U.S.C. § 841(a)(1), distribution of a controlled substance. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. The purpose of this Affidavit is to support a criminal complaint naming, and an arrest warrant for, **ISHO**, as well as three search and seizure warrants for the residence and vehicles described in Attachments A-1, A-2, and A-3, to include:

A. 2304 Quail Meadow Drive, Modesto, California 95355 (hereafter referred to as **SUBJECT RESIDENCE 1**), further described in Attachment A-1; and

B. a black Lincoln MKZ Sedan bearing California license plate 7ZSM535, (hereafter referred to as **SUBJECT VEHICLE 1**), further described in Attachment A-2; and

C. a gold GMC Yukon SUV bearing California license plate DISNYCA, (hereafter referred to as **SUBJECT VEHICLE 2**), further described in Attachment A-3; and

As well as the seizure of **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2** and all items described in Attachment B.

III. TECHNICAL BAKCGROUND

6. Digital currency (also known as crypto-currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government.) Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

7. Bitcoin is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification, and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

8. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

9. Bitcoins can be stored in digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private key is like the password to access that account.

10. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public

addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

11. Through the dark web or darknet, i.e. websites accessible only through encrypted means, individuals have established online marketplaces, such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through digital currencies, such as Bitcoin. Accordingly, a large amount of Bitcoin sales or purchases by an individual is often an indicator that the individual is involved in narcotics trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoin as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoin to convert them to legal tender. Such purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers who advertise their services on websites designed to facilitate such transactions.

12. Dark web sites (such as Dream, Wall Street, and Silk Road 3.1) operate on "The Onion Router" or "TOR" network. The TOR network ("TOR") is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. TOR likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the TOR network. Such "hidden services" operating on TOR have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the TOR network.

///

///

IV. SUMMARY OF THE INVESTIGATION

13. Members of the Northern California Illicit Digital Economy ("NCIDE") task force, which is composed of the U.S. Postal Inspection Service ("USPIS"), Homeland Security Investigations ("HSI"), the Federal Bureau of Investigation ("FBI"), and the Drug Enforcement Administration ("DEA"), investigated this case. As a function of this task force, investigators regularly purchase narcotics utilizing both digital and legal tender, from the persons operating and illegally selling narcotics from the "dark" portion of the internet and from various social media platforms. Investigators regularly conduct undercover purchases of narcotics in an effort to assist in identifying the suspects operating such illicit sites. Additionally, investigators routinely profile parcels within the US Mail stream, looking for links to dark web narcotics vendors.

14. During this investigation, federal law enforcement officers have: (1) observed **ISHO** place parcels believed to contain methamphetamine into the United States Postal Service ("USPS") mail system; and (2) conducted undercover purchases of methamphetamine from online accounts believed to be operated by **ISHO**. In doing so, **ISHO** is believed to be distributing a controlled substance, in violation of 21 U.S.C. § 841(a)(1), which states "it shall be unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance."

V. FACTS ESTABLISHING PROABLE CAUSE

A. *Case Initiation*

14. Beginning on or about 2017, case agents began reviewing USPS shipping records for the purpose of investigating dark web vendors in the Northern California area selling illegal narcotics. As part of the investigation, case agents reviewed shipping records of numerous persons who offer "cash-in-mail" (CIM) services in exchange for the purchase of bitcoin. When

reviewing the records, case agents observed there was an individual operating out of the Modesto, California area who was receiving a large amount of suspected CIM parcels. Case agents observed the male, identified as **ISHO**, had received well over twenty (20) suspected CIM parcels between early 2016 and 2017. The parcels were received at three separate addresses: P.O. Box 844, Modesto, CA 95353; 2304 Quail Meadow Drive, Modesto, California 95355 (**SUBJECT RESIDENCE 1**); and 2601 Oakdale Road, Suite H2 Box 213, Modesto, CA 95355.

15. Case agents conducted a check of Thomson Reuters CLEAR and USPS records and determined that **ISHO** was associated with each of the three mailing addresses at the time CIM parcels were being delivered to the addresses. In January 2018, **ISHO** closed down the private mailbox rental on Oakdale Road and no future parcels were delivered to that address after that date. In late 2018, case agents again checked CLEAR and observed **ISHO** was still associated with the PO Box 844 and **SUBJECT RESIDENCE 1**, and he was also now associated with an additional address: 1243 Lauralee Court, Modesto, CA 95350.

B. *Dark Web Vendor "Bulletproof-packs" on DREAM Market*

16. On January 22, 2018, Bulletproof-packs (BPP) joined the Dream Market (DREAM). BBP ceased being active on February 17, 2019. During this time period, BPP earned 1,750 customer reviews with a 4.95 out of 5.0 star possible rating. BBP's advertisement included a Pretty Good Privacy (PGP) key. PGP is an encryption program that provides cryptographic privacy and authentication for data communication. PGP makes use of public-key encryption, in which one key is used to encrypt the data (the public key) and another key is used to decrypt it (the private key). This technology allows, for example, a dark-web drug vendor to communicate in an encrypted format by broadcasting his/her public key to customers who can then encrypt messages they want to send to the vendor. BPP's PGP key was created on January 22, 2018, and had a fingerprint ID of 672F A621 EE20 AF9C C02A 97E2 231A AE22 0B60 60FC.

17. BPP offered for sale various marijuana products in quantities ranging from one gram to one pound. BPP temporarily offered for sale methamphetamine in gram quantities, but removed the listings sometime in January 2019. BPP also had a "Tip Jar" listing for $2.08. I believe, based on what I have learned over the course of this investigation, and my conversations with other law enforcement agents, that the "Tip Jar" listing was created as a way for customers to pay BPP extra in exchange for better service. For example, a customer buying illegal narcotics could also buy a tip with the expectation of faster shipping.

18. In November 2018, law enforcement in Pittsburgh, Pennsylvania, conducted an undercover buy of methamphetamine on DREAM from the dark web vendor BPP. On November 29, 2018, the parcel associated with the undercover buy was delivered. The parcel was a small flat rate box bearing tracking number 9114 9014 9645 0935 3263 13 and had the return name "CPUTech 15960 Bizzibe St. Lathrop, CA 95330" on it. The parcel contained a priority mail stamp and a forever stamp. Upon opening the parcel, law enforcement discovered it contained a 1,000 piece puzzle box. Inside the puzzle box, there were puzzle pieces wrapped in clear plastic. Also in the clear plastic with the puzzle pieces, was a silver colored foil pouch. Inside the foil pouch, was a bag containing what appeared to be methamphetamine. The suspected methamphetamine weighed approximately 8 grams (weight including packaging). A check of USPS records, using the parcel's tracking number, confirmed the parcel was mailed from a post office in the Eastern District of California.

19. In December 2018, law enforcement in Pittsburgh Pennsylvania, conducted another undercover buy of methamphetamine on DREAM from BPP. On December 20, 2018, the parcel associated with the undercover buy was delivered. The parcel was a small flat rate box bearing tracking number 9114 9014 9645 0935 3165 43 and had the return name "CPUTech 7674 Jasmine Ct Dublin, CA 94568" on it. The parcel contained a priority mail stamp and forever stamp as postage, like the previous BPP methamphetamine parcel. Upon opening the parcel, law enforcement discovered it contained a 300 piece puzzle box. Inside the puzzle box,

there were puzzle pieces wrapped in clear plastic. Also in the clear plastic with the puzzle pieces, was a silver colored foil pouch. Inside the foil pouch, was a bag containing approximately 8 grams of methamphetamine (weight includes packaging). A check of USPS records, using the parcel's tracking number, confirmed the parcel was mailed from a post office in the Eastern District of California.

C. *Large Stamp Purchases and Identification of Omar Isho*

20. In December 2018, case agents conducted a detailed search of USPS records and databases, looking for any large cash purchases in the greater Stockton and Modesto, California areas, of the specific type of priority mail stamps used on the Bulletproof-packs parcels. Law enforcement found that the French Camp Post Office, located at 315 E. French Camp Rd, French Camp, CA 95231, was the only post office in the area where persons using cash made regular, large purchases of the priority mail stamps. Specifically, U.S. Postal Inspectors observed that on November 5th, November 20th, December 4th, December 10th and December 17th, 2018, large purchases of the priority mail stamps were all made at the French Camp Post Office, totaling over $2,000.00 in priority mail postage ~~between those five days.~~

21. On December 20, 2018, case agents contacted the Postmaster of the French Camp Post Office and inquired about the large stamp purchases. Postmaster Mondragon immediately stated he knew the person agents were inquiring about. Mondragon stated it was always the same person who purchased the stamps and he knows the male only by the name "Rome". Mondragon stated "Rome", later determined to be **ISHO**, comes in about once a week, purchases large amounts of the priority stamps, along with large numbers of the forever stamps and always conducts the transactions in cash. Additionally, **ISHO** often asks for additional stacks of priority mail flat rate boxes (the same one used during the BPP buys) and additional pads[1] of Priority

[1] Generally, when stamps are used as postage, like on these packages, there is no way to track the package; but these sticky pads have preprinted tracking numbers on them, which then provide a way to track the parcels.

Mail tracking numbers (also used on the BPP buys). Mondragon described **ISHO** as a male, approximately 40 years old, with a thick build and a shaved head. Mondragon advised **ISHO** drove an unknown type of black car. On December 20, 2018, case agents reviewed the French Camp Post Office surveillance video recorded during the times the stamp purchases were made on the five days mentioned above, and observed it was the same male conducting all five purchases.

22. On December 20, 2018, following the review of the surveillance images from the French Camp Post Office, case agents asked Postmaster Mondragon to put aside 5 pads of the priority mail tracking numbers and advised him the next time **ISHO** came to the post office and asked for additional pads of tracking numbers, to give him the five pads. Postmaster Mondragon photo documented the five pads of tracking numbers and sent images of them to case agents. Case agents also asked the staff at the French Camp Post Office to attempt to get a further description of the vehicle driven by **ISHO** the next time he came in.

23. On December 27, 2018, case agents were notified by Postmaster Mondragon that **ISHO** came into the post office, bought another large volume of stamps and asked for more pads of tracking numbers. Postmaster Mondragon advised after **ISHO** purchased the stamps, a member of his staff provided **ISHO** with the five pads of "bait" tracking numbers as requested. In addition, after **ISHO** departed the post office, one member of the staff surreptitiously took a photo of the black vehicle he was driving as it was departing the parking lot (**SUBJECT VEHICLE 1**). Case agents conducted a later review of the post office surveillance video and confirmed the male was the same male who had come in on all the previously mentioned occasions.

24. **SUBJECT VEHICLE 1** is a black 2014 Lincoln 4-door sedan with California license plate number 7ZSM535 and VIN 3LN6L2GK5ER809145. On December 27, 2018, case agents conducted a check of the registration on the license plate and found the registered owner to be listed as: WUNSCH, Ashley Lynn, 1243 Lauralee Ct Modesto, CA 95350. Case agents

immediately recognized the registered owner address as that belonging to **ISHO**, from the prior CIM investigation. A check of California DMV records, as well as of numerous open source social media sites involving WUNSCH and **ISHO**, and positively identified **ISHO** as the male routinely buying the large volumes of priority mail and forever stamps at the French Camp Post Office. The registered owner of the vehicle, WUNSCH, was identified as **ISHO**'s spouse. A check of law enforcement databases and social media sites, identified prior aliases belonging to ISHO as "Rome", "Romeo" and "Ramon". These names are similar to the name by which Postmaster Mondragon knows **ISHO**, which is "Rome."

25. On January 7, 2019, case agents conducted searches in USPS databases of the bait tracking numbers given to **ISHO**, to determine if any of the bait tracking numbers had entered the mail stream. Your affiant learned the first tracking number on one of the pads (Priority Mail 9114 9014 9645 0848 5450 23) had been used on a small flat rate parcel mailed out of a Ceres, California post office on December 28, 2018, the day after **ISHO** received the bait tracking pads. Based on a photo of the parcel contained in USPS databases, it looked nearly identical to the other parcels received as a result of the BPP undercover methamphetamine buys conducted by law enforcement. The return address on the parcel was listed as: "CPUTech, 415 N Minaret Ave. Turlock, CA 95380, which is the same sender name (CPUTech), but not the same address, that was used by BPP on his parcels to undercover law enforcement.

D. *Dark Web Vendor "DrFrosty" on DREAM*

26. Vendor DrFrosty joined DREAM on January 9, 2018 and was active until March 2019. During this time, DrFrosty earned 1,300 customer based reviews, with a 4.94 out of 5.0 star rating. DrFrosty displayed a PGP key, created on February 14, 2018, that bore the email address of "DrFrosty@secmail.pro" and the fingerprint ID: 9AAD D187 1050 C11F 957A 27B8 8E3B 4CEF 7662 5610. DrFrosty had listings of methamphetamine and marijuana products for sale. The methamphetamine listings range from one gram to one half pound and the marijuana

listings range from one gram to one pound. DrFrosty had two "speed ball" listings (one gram and three and one half grams) which were described as a mixture of cocaine and methamphetamine. DrFrosty also has a "Tip Jar" listing for $2.08.

27. In January 2019, law enforcement in Pittsburgh, Pennsylvania, conducted another undercover buy of methamphetamine on DREAM, this time from the vendor "DrFrosty". On January 18, 2019, the parcel associated with the undercover buy was delivered. The parcel was a small flat rate box bearing tracking number 9505 5152 5147 9015 1770 09 and the return name "CPUTech 1505 N Stockton St. Stockton, CA 95203". Upon opening the parcel, law enforcement discovered it contained a 300 piece puzzle box. Inside the puzzle box, there were puzzle pieces wrapped in clear plastic. Also in the clear plastic with the puzzle pieces, was a silver colored foil pouch. Inside the foil pouch, was a bag containing approximately 8 grams of methamphetamine (weight includes packaging). A check of USPS records confirmed the parcel was mailed from the a post office located at 3333 E Main St, Stockton, CA 95205, along with ten other similar parcels, on January 15, 2019.

28. On January 29, 2019, case agents reviewed and downloaded surveillance video from the East Stockton post office at the time of the January 15th mailings. The review of the video confirmed the person mailing the "DrFrosty" methamphetamine buy parcel, along with 10 other parcels, was **ISHO**.

E. *DrFrosty on the Wall Street, Empire and Silk Road 3.1 Markets*

29. Following the identification of the DrFrosty account on the DREAM market, case agents conducted additional research of other dark web markets, and identified DrFrosty was an active vendor on three additional markets under the exact same name, using the same PGP key, and offering nearly identical products as those listed on DREAM. DrFrosty joined the Wall Street Market (WSM) on October 2, 2017 and was active until April 2019. During that time, DrFrosty earned over 960 customer reviews, with a 4.87 out of a 5.0 star rating. DrFrosty joined

the Empire Market on February 19, 2018 and is still active on the market place. During this time period, DrFrosty earned over 400 customer reviews, with a 99% positive rating. DrFrosty joined the Silk Road 3.1 Market in 2018 (the market does not specify the exact date of establishment) and is still active on the marketplace. During this time, DrFrosty earned +291 and -0 customer reviews, with a 100% positive rating.

F. *Surveillance of 1243 Lauralee Court on February 1, 2019*

30. On February 1, 2019, case agents established surveillance in the vicinity of one of **ISHO**'s listed residences, 1243 Lauralee Court, Modesto, CA. No vehicles were observed at the initiation of the surveillance. At approximately 11:15 a.m., while law enforcement was parked in the vicinity of the Lauralee Court residence, **SUBJECT VEHICLE 1** entered the Lauralee Court. **SUBJECT VEHICLE 1**, driven by **ISHO**, approached the unmarked law enforcement vehicle, parked next to it for approximately ten seconds and then departed the neighborhood. **ISHO** never stopped at the Lauralee residence.

G. *Undercover Purchase from "DrFrosty" on February 9, 2019*

31. On February 9, 2019, law enforcement in Sacramento, California ordered methamphetamine from dark web vendor "DrFrosty" on DREAM. On February 14, 2019, the parcel associated with the undercover buy, was delivered to the undercover address in Sacramento, California, controlled by law enforcement. The parcel was a small flat rate Priority Mail box bearing tracking number 9114 9014 9645 0848 5490 45, which contained a priority mail and forever stamp in the upper right corner. The sender information on the parcel was on a preprinted sticker which listed the sender as "PZQ 1718 E. Hazelton Ave. Stockton, CA 95202". Upon opening the parcel, law enforcement discovered it contained a 500 piece puzzle box. Inside the puzzle box, Inspectors observed a plastic bag containing puzzle pieces, with a silver foil pouch concealed within. Inside the foil pouch, was a clear plastic baggie containing clear crystalline shards, which field tested positive for methamphetamine. The suspected

methamphetamine weighed approximately 2 grams with packaging.

H. ***Surveillance of SUBJECT RESDIENCE 1 on February 11, 2019***

32. On February 11, 2019, case agents established surveillance in the vicinity of **SUBJECT RESIDENCE 1**, the likely residence of **ISHO** and WUNSCH. Parked in the driveway at the time, were both **SUBJECT VEHICLE 1** and a gold GMC SUV bearing California personalized license plate DISNYCA (**SUBJECT VEHICLE 2**). A check of the registered owner of **SUBJECT VEHICLE 2** produced the following information: 2013 GMC with VIN: 1GKS2CE09DR239291, with registered owner WUNSCH, Ashley Lynn, 1243 Lauralee CT, Modesto 95350. At approximately 11:20 a.m., agents observed **ISHO** depart the residence driving **SUBJECT VEHICLE 1**. Mobile surveillance was initiated and case agents followed **ISHO** until he drove into Lauralee Court. Due to the court being a dead end and due to **ISHO**'s behavior during the previous surveillance, agents did not follow him into the dead end court. Approximately nine minutes later, **ISHO** departed the neighborhood and was followed back to the Quail Meadow residence.

33. At approximately 2:30 p.m., **SUBJECT VEHICLE 1** again departed the residence, with **ISHO** as the driver and WUNSCH as the passenger. A short time later, WUNSCH, **ISHO** and a juvenile child were seen entering a nearby gym. Approximately one and one half hour later, the three exited the gym, and entered into **SUBJECT VEHICLE 1**, this time with WUNSCH as the driver and **ISHO** as the passenger. Mobile surveillance was again established and followed **SUBJECT VEHICLE 1** until it arrived at the parking lot of the Dollar Tree, located at 2425 B McHenry Ave, Modesto, CA. **ISHO** exited the vehicle and entered into the Dollar Tree store. Law enforcement continued surveillance of **ISHO** inside the store and observed as he purchased what was estimated to be approximately forty (40) puzzles, which appeared to be the same type used in all of the previously observed methamphetamine buy

parcels. Following the purchase, **ISHO** placed the puzzles in the front passenger seat of the vehicle and WUNSCH drove them back to **SUBJECT RESIDENCE 1**.

I. *Undercover Purchases from "DrFrosty", February 24-26, 2019*

34. On February 24, 2019, law enforcement in Sacramento, California conducted an undercover purchase of methamphetamine from the dark web vendor "DrFrosty" on the Empire Market. As with the previous undercover purchases, DrFrosty was instructed to ship the parcel to an address that is controlled by law enforcement.

35. On February 25, 2019, law enforcement in Sacramento, California conducted an undercover purchase of methamphetamine from the dark web vendor "DrFrosty" on the Silk Road 3.1 Market. During the buy, DrFrosty was instructed to ship the parcel to an undercover address controlled by law enforcement.

36. On February 26, 2019, law enforcement in Sacramento, California conducted an undercover purchase of methamphetamine from the dark web vendor "DrFrosty" on the Wall Street Market. During the buy, DrFrosty was instructed to ship the parcel to an undercover address controlled by law enforcement.

J. *SUBJECT RESIDENCE 1 trash pull on February 27, 2019*

37. On February 27, 2019, law enforcement surreptitiously looked through the garbage in the city trash cans on the curb outside the **SUBJECT RESIDENCE 1**. Located within the trash cans, case agents observed items of indicia bearing the names of **ISHO** and WUNSCH. These items included a financial document with **ISHO**'s name at the P.O. Box 844 address; a financial document with WUNSCH's name at the Lauralee Court address; an old parcel with WUNSCH's name at **SUBJECT RESIDENCE 1**; and a snow sports form with **ISHO**'s name and the P.O. Box 844 address. In addition, agents located numerous puzzle pieces

and puzzle boxes, that appeared similar to those bought by ISHO at the Dollar Tree on February 11 and those used to ship the numerous undercover buy parcels.

K. *Surveillance of SUBJECT RESDIENCE 1 on February 28, 2019*

38. On February 28, 2019, case agents conducted surveillance at **SUBJECT RESIDENCE 1.** At the initiation of the surveillance, **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2** were both parked at the residence. During the surveillance, case agents observed WUNSCH and ISHO both separately driving **SUBJECT VEHICLE 1**.

L. *Mailing of the February 24-26, 2018 UC buy parcels by ISHO*

39. On March 2, 2019, all three parcels associated with February 24th, 25th, and 26th undercover methamphetamine buys, entered the US Mail stream. On March 6, 2019, case agents received and opened all three parcels. All three parcels were nearly identical in nature to each other and to previous packages ordered by undercover law enforcement in Pittsburgh and Sacramento. All three parcels were USPS Priority Mail small flat rate boxes and bore identical preprinted stickers bearing the sender name and address of "PZQ 2960 James M Wood Blvd. Los Angeles, Ca 90006". The recipient name and address on each parcel was also preprinted on a sticker, as seen on other parcels in this investigation. All three parcels contained puzzle boxes, with methamphetamine concealed inside the puzzle pieces. A check of USPS records, confirmed the three parcels were all mailed at separate post offices, located throughout the central valley of California. Most noteworthy, law enforcement observed the parcel associated with the February 24th undercover methamphetamine buy from the Empire market (with USPS Priority Mail tracking number 9505 5138 1876 9061 2518 04), was mailed at the Post Office located at 6301 Olive Avenue, Fresno, CA 93701. Law enforcement reviewed the surveillance video recorded at the Fresno Post Office at the time of the mailing and observed the person mailing the parcel, along with nine other similar parcels, was **ISHO**.

40. On March 18, 2019, case agents conducted a review of USPS records and databases and observed that on March 6, 2019, four parcels with similar appearances to the other DrFrosty parcels identified in this investigation, were mailed from the post office located at 4245 West Lane, Stockton, CA 95208. The four parcels each bore a preprinted sticker with the sender name and address of "PZQ 1505 N Stockton St. Stockton, CA 95203". The USPS records indicated the parcels were "accepted" by the USPS on March 6, 2019 at approximately 5:23 p.m., and were likely mailed from a blue collection box located at the post office. Also on March 18, 2019, case agents reviewed post office surveillance video recorded at the time the four parcels were mailed. During the video review, case agents observed that, less than one hour before the parcels were accepted by the USPS, **SUBJECT VEHICLE 2** was observed parked in the post office parking lot. Case agents further observed ISHO exit the passenger seat of **SUBJECT VEHICLE 2** carrying a white grocery bag and deposited a number of parcels into the post office blue collection box. After mailing the parcels, **ISHO** entered the passenger seat of **SUBJECT VEHICLE 2** and it departed the post office lot. As the vehicle exited the lot, the surveillance camera was at such an angle, that the face of the driver of **SUBJECT VEHICLE 2** could not be observed, but it seemed apparent the driver was a female, and had similar hair, skin tone and build as WUNSCH. During the length of this ongoing investigation, no other persons besides WUNSCH and **ISHO** have been observed driving **SUBJECT VEHICLE 2**.

M. ***Tracker warrants on SUBJECT VEHICLES 1 and 2***

41. On March 21, 2019, the Honorable Deborah Barnes, of the Eastern District of California, authorized federal tracking warrants (2:19-SW-230-DB and 2:19-SW-231-DB) for **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2**, operated by **ISHO** and WUNSCH. On March 27, 2019, law enforcement installed an electronic tracking device on **SUBECET VEHICLE 2**. On March 28, 2019, law enforcement installed an electronic tracking device on **SUBJECT VEHICLE 1**.

42. Following the installation of the tracking devices, law enforcement observed that

SUBJECT VEHICLE 1 and **SUBJECT VEHICLE 2** regularly visit post offices, often times, visiting multiple different post offices on the same day.

43. On March 29, 2019, a review of tracker data showed **SUBJECT VEHICLE 2** visited multiple post offices. A later check of USPS records and databases located multiple parcels were mailed from the visited post offices, that were nearly identical to the numerous undercover methamphetamine buy parcels observed in this investigation. The parcels mailed on this day, bore the fictitious sender business name of "PZQ".

44. On April 1st, 3rd, 5th and 10th, 2019, a review of the tracker data showed **SUBJECT VEHICLE 1** visited multiple post offices on each of the days. Following the departure of the Lincoln from the various post offices, law enforcement verified within minutes of the Lincoln departing, multiple parcels had been mailed by **ISHO**, that were nearly identical to the numerous undercover meth buy parcels observed in this investigation. The dozens of parcels mailed by **ISHO** on the days mentioned above, bore the fictitious sender business names of "PZQ" and "CP Tech".

45. On May 2, 2019 at approximately 4:00 a.m., law enforcement agents observed **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2** parked in front of the driveway of the **SUBJECT RESIDENCE 1**. Based on a review of the tracker data, **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2**, continue to be driven by **ISHO** and WUNSCH and continue to be regularly parked during overnight hours at **SUBJECT RESIDENCE 1**.

N. *Undercover Purchase and ISHO Mailing at the Hayward Post Office*

46. On April 2, 2019, law enforcement in Sacramento, California conducted an undercover purchase of two ounces of methamphetamine from dark web vendor "DrFrosty" on the Wall Street Market. On April 11, 2019, law enforcement was real-time monitoring the tracker installed on **SUBJECT VEHICLE 1**. Law enforcement observed the tracker departed **SUBJECT RESIDENCE 1** and travelled until it stopped for brief periods at a post office located in Castro Valley, California and a post office located in Hayward, California. Within

minutes of the tracker data showing **SUBJECT VEHICLE 1** departed the two post offices, law enforcement confirmed multiple parcels similar to the others identified in this investigation, were mailed from the post offices. Upon further inspection of the parcels mailed from the Hayward Post Office, law enforcement observed the parcel bearing tracking number 9114 9014 9645 0848 5608 35, was addressed to the undercover name and address utilized by law enforcement during the recent undercover buy of methamphetamine. The sender information on the parcel was on a preprinted sticker which listed the sender as "CP Tech 728 Diamond St. San Francisco, CA 94114". Upon opening the parcel, law enforcement discovered it contained a 1,000 piece puzzle box. Inside the puzzle box, Inspectors observed a plastic bag containing puzzle pieces, with a silver foil pouch concealed within. Inside the foil pouch, was a clear plastic baggie containing clear crystalline shards, which field tested positive for methamphetamine. The suspected methamphetamine weighed approximately 31 grams with packaging.

O. ***Seizure of "cash-in-mail" parcel destined for ISHO***

47. On April 4, 2019, law enforcement intercepted a parcel destined to "OMAR ISHO PO BOX 844 MODESTO CA 95353-0844". The sender information listed on the parcel, was that of a previously identified individual who sends large volumes of "cash-in-mail" parcels to customers, in exchange for bitcoin. On April 24, 2019, the Honorable Carolyn K. Delaney authorized a federal search warrant for the parcel (2:19-SW-0350-CKD). On April 24, 2019, law enforcement executed the search warrant and opened the parcel. As a result, law enforcement seized from the parcel, $9,142.00 in US Currency, concealed within numerous layers of packaging. A sticker with preprinted writing was affixed to the money packaging inside the parcel which read "$9142 FOR 2 BTC".

48. I believe based on my training and experience, what I have learned over the course of this investigation, and my conversations with other law enforcement officers, that this writing indicates that the sender is sending $9,142 cash in exchange for 2 bitcoin. I also believe that **ISHO** likely exchanged 2 bitcoin, from sales of illegal narcotics on the dark web, for more

usable U.S. currency, using this CIM service.

P. *Undercover Purchase and ISHO Mailing at Stockton Post Offices*

49. On May 13, 2019, law enforcement in Sacramento, California conducted an undercover purchase of methamphetamine from dark web vendor "DrFrosty" on Silk Road 3.1. On May 15, 2019, law enforcement was real-time monitoring the tracker installed on **SUBJECT VEHICLE 1**. Law enforcement observed the tracker departed **SUBJECT RESIDENCE 1** and travelled until it stopped for brief periods at a post offices located in Stockton, California. Within minutes of the tracker data showing **SUBJECT VEHICLE 1** departed the two post offices, law enforcement confirmed multiple parcels similar to the others identified in this investigation, were mailed from the post offices. Upon further inspection of the parcels mailed from the Stockton Hammer Ranch Post Office, law enforcement observed the parcel bearing tracking number 9114 9014 9645 0320 8007 70, was addressed to the undercover name and address utilized by law enforcement during the recent undercover buy of methamphetamine. The sender information on the parcel was on a preprinted sticker which listed the sender as "PZQ 1505 N Stockton St. Stockton, CA 95203". Upon opening the parcel, law enforcement discovered it contained a 500 piece puzzle box. Inside the puzzle box, Inspectors observed a plastic bag containing puzzle pieces, with two silver foil pouches concealed within. Inside each foil pouch, was a clear plastic baggie containing clear crystalline shards, which field tested positive for methamphetamine. Both baggies of suspected methamphetamine were weighed together totaling approximately 9 grams with packaging.

VI. SEARCH OF DIGITAL INFORMATION

50. Your affiant is aware that vendors of narcotics on the Internet use a computers, including smart phones, to access the web and conduct narcotic sales. Your affiant is also aware that individuals must use an electronic device to locate and communicate with bitcoin exchangers and purchase bitcoins.

Users of bitcoin must establish electronic wallets to receive and send bitcoins. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, and/or computers. Your affiant is aware that once contact is made with a bitcoin exchanger on a digital currency exchange platform, all subsequent contact and transactions can be conducted from one phone to the other during a face to face transaction, exchanging currency for bitcoins. Your affiant is also aware that users can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access electronic wallets, are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. There is probable cause to believe that such items are located in **SUBJECT RESIDENCE 1**, in **SUBJECT VEHICLES 1 and 2**, and on **ISHO**'s person.

51. As described above and in Attachment B, your affiant submits that computers, smart phones, and possibly other storage media will likely be found within **SUBJECT RESIDENCE 1**, in **SUBJECT VEHICLES 1 and 2,** and on **ISHO**'s person, and there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. Furthermore, your affiant submits that sufficient probable cause has been established to search and seize any online digital currency exchange platform accounts, and the data contained therein, located on seized digital devices.

52. For example, based on my knowledge, training, and experience, your affiant is aware that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

53. Based on my knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little to no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because 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 storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

54. Also, again based on your affiant's training and experience, wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium 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). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

55. As further described in Attachment B, this application seeks permission to locate not only

computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

56. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

57. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving interstate drug sales and movement of drug proceeds. Devices such as modems and routers can contain information about dates, frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

58. Similarly, files related to the purchasing and selling of controlled substances, as well as, the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or "cache". The browser often 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 viewed internet pages or if a user takes steps to delete them. 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.

59. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Your affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

60. Searching computers for evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

61. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and

completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

62. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

63. The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

64. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the

storage media off- site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

65. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VII. REQUEST FOR SEALING

66. I request that the Court seal the warrant and the affidavit and application in support thereof, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office and may be served on Special Agents and other investigative and law enforcement officers of USPIS, HSI, DEA, and FBI, and federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, as necessary to effectuate the warrant. These documents pertain to and discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation.

67. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation. Sealing these documents will also better ensure the safety of agents and others.

VIII. CONCLUSION

68. Based on the facts set forth in this Affidavit, I believe there is probable cause that evidence, fruits, proceeds, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance) are concealed in the locations identified in Attachments A-1, A-2, and A-3. Accordingly, I respectfully request the issuance of a search warrant authorizing the search of the locations described in Attachments A-1, A-2 and A-3, as well as the seizure of items described in Attachment B.

69. Furthermore, I believe that there is probable cause that **OMAR ISHO** committed the same crime, thus supporting the legal basis for the Court to issue an arrest warrant based on a criminal complaint.

Respectfully submitted,

Andrew Cornwell
United States Postal Inspector

Subscribed and sworn to before me on: 5/21/2019

The Honorable Carolyn K. Delaney
UNITED STATES MAGISTRATE JUDGE

Approved as to form
QUINN HOCHHALTER

ATTACHMENT A-1

The **SUBJECT RESIDENCE 1** to be searched pursuant to the requested warrant is described as follows:

The residence located at 2304 Quail Meadow Drive, Modesto, CA 95355

The residence is further described as a single family residence, which is located on the south side of Quail Meadow Drive right before entering Quail Meadow Court. The residence is an approximately 1,400 sq. ft., single story residence which is light beige in color, stucco construction, with brown trim, red brick accents and a brown shingle roof. There is a standard two car garage door that is white in color, which faces Quail Meadow Drive. As you face the residence, to the right of the garage door are the white colored numbers "2304" affixed to the house in a vertical pattern. Immediately to the right of the garage, set back a few feet, is the front door. The rear and portions of the sides of residence are surrounded by an approximately six foot tall, wooden privacy fence.

The search is to include:

ANY AND ALL locked or closed rooms, closets, safes, cabinets, and hidden compartments within the residence and any sheds or storage facilities on the property.

ATTACHMENT A-2

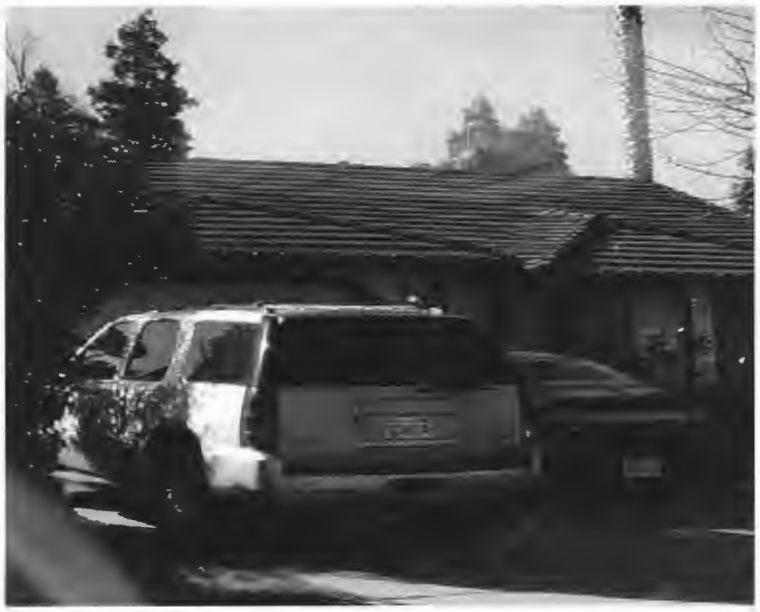
The **SUBJECT VEHICLE 1** to be searched pursuant to the requested warrant is described as follows:

A black 2014 Lincoln MKZ sedan bearing California license plate 7ZSM535 and Vehicle Identification Number 3LN6L2GK5ER809145

The search is to include:

ANY AND ALL locked or closed safes, glove boxes, hidden compartments or storage compartments, bags, or other containers within the vehicle.

ATTACHMENT A-3



The **SUBJECT VEHICLE 2** to be searched pursuant to the requested search warrant is described as follows:

A gold 2013 GMC Yukon SUV bearing California license plate DISNYCA and Vehicle Identification Number 1GKS2CE09DR239291

The search is to include:

ANY AND ALL locked or closed safes, glove boxes, hidden compartments or storage compartments, bags, or other containers within the vehicle.

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as computers, hard drives, flash drives, tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute or contain evidence, instrumentalities, or fruits of violations of 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance):

1. All records relating to the violations described above, including:
   a. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of controlled substances;
   b. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of packaging materials;
   c. any and all documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;
   d. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;
   e. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;
   f. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;
   g. any and all records or other items which are evidence of ownership or use

of computer equipment, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.

h. any and all records relating to indicia of occupancy, residency, and ownership or use of the locations described in Attachments A-1, A-2, and A-3, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys;

i. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of controlled substances and/or virtual currency, identifying information for customers purchasing controlled substances and/or virtual currency;

j. all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

k. all copies of income tax returns filed with the Internal Revenue Service (IRS) or the California Franchise Tax Board;

l. all records related to the purchase of real estate or other assets, or the leasing of storage units,

m. financial records for OMAR ISHO and ASHLEY WUNSCH, including foreign and domestic banking records, ledger books, wire transfer instructions, and receipts for wire transfers,

n. bulk cash in excess of $1,000.

2. Any digital devices or other electronic storage media and/or their components used as a means to commit the violation described above, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the offenses listed above;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including

word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media 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, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other

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

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of 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.

5. Any and all encrypted chat applications used in furtherance of the offenses described above.

6. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above.

7. Virtual currency in any format, including but not limited to, wallets (digital and paper), seed words, usernames and passwords, public keys (addresses) and private keys.

8. Fiat currency (U.S. dollars or other government issued currency).

9. Keys to storage units, suites, lockers and safe deposit boxes.

10. Firearms or other prohibited weapons.

11. Controlled substances and associated paraphernalia.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME