AO 91 (Rev. 11/11) Criminal Complaint

REDACTED

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED
MAY 21 2018
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY DEPUTY CLERK

United States of America
v.

JOSE ROBERT PORRAS III, and
PASIA VUE.

Case No. 2:18-MJ-0102 CKD

Defendant(s)

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 August 2017 – May 2018 in the county of Sacramento in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1) & (b)(1)(C)	Drug Distribution
21 U.S.C. §§ 846 and 841(a)(1) & (b)(1)(C)	Drug Distribution Conspiracy
18 U.S.C. §§ 1956 and 1957	Money Laundering

This criminal complaint is based on these facts:

See attached Affidavit of Aron Mann.

☒ Continued on the attached sheet.

Complainant's signature

Aron Mann, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/21/2018

Judge's signature

City and state: Sacramento, California

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

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANT

I, Aron Mann, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2016. As a requirement for employment as an HSI Special Agent, I successfully completed the Criminal Investigator Training Program ("CITP") located at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. At the conclusion of CITP, I completed an additional Homeland Security Investigations Special Agent Training Academy. As part of the training at FLETC, I received extensive instruction in the areas of immigration law, customs law, illegal narcotics, firearms, surveillance, and interview techniques.

2. As a Special Agent with HSI, part of my duties include the investigation of criminal violations as proscribed by 21 U.S.C § 841 (narcotics trafficking) and 21 U.S.C § 846 (drug conspiracy). Moreover, as an HSI Special Agent, I am a "Federal Law Enforcement Officer," authorized to investigate violations of the laws of the United States and to execute search and seizure warrants issued under the authority of the United States.

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

II. PURPOSE

4. 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. Rather, I make this affidavit in support of an application for a warrant to search:

(1) 1066 O'Donnell Avenue, Sacramento, California 95838 (hereafter referred to as the SUBJECT PREMISES), further described in Attachment A-1;

(2) 3300 Northgate Boulevard, Unit E196, Sacramento, California 95834 (hereafter referred to as the STORAGE UNIT), further described in Attachment A-2;

(3) a 2013 Mercedes-Benz S550, California license plate 7ZIV981, bearing Vehicle Identification Number WDDNG9EB8DA505449 (hereafter referred to as the SUBJECT VEHICLE), further described in Attachment A-3;

the seizure of the SUBJECT VEHICLE;

the seizure of the items described in Attachment B;

and,

a criminal complaint naming JOSE ROBERT PORRAS III and PASIA VUE.

For violations of:

a. Title 21 U.S.C. § 841(a)(1) (Manufacture or Distribution of a Controlled Substance);

b. Title 21 U.S.C. § 846 (Conspiracy to Manufacture, to Distribute, and to Possess with Intent to Distribute a Controlled Substance); and,

c. Title 18 U.S.C. § 1956 & 1957 (Money Laundering and Conspiracy).

III. OVERVIEW

5. During this investigation, Federal Law Enforcement Officers have: observed JOSE ROBERT PORRAS III ("PORRAS"), a/k/a CANNA_BARS and THEFASTPLUG, and his girlfriend PASIA VUE ("VUE"), place suspected narcotics parcels into the United States Postal Service ("USPS") mail system; [redacted]; observed PORRAS and VUE using a leased storage unit to store and package narcotics and store the proceeds of narcotics sales; and, conducted two undercover purchases of marijuana from PORRAS. In doing so, PORRAS and VUE are:

a. Manufacturing and distributing controlled substances.

i. Under 21 U.S.C. § 841(a)(1), "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."

b. Conspiring to manufacture and distribute controlled substances.

i. Under 21 U.S.C. § 846, "any person who attempts or conspires to commit any offense defined in this subchapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy."

c. Laundering monetary instruments.

i. Under 18 U.S.C. § 1956, "Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds or specified unlawful activity; or to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both."

d. Engaging in monetary transactions in property derived from specified unlawful activity.

i. Under 18 U.S.C. § 1957, "Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b)."

IV. TECHNICAL BACKGROUND

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 fiat

(government-backed) currency. 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 Silk Road, AlphaBay, and Dream, 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, which are many times generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the TOR network.

V. FACTS ESTABLISHING PROBABLE CAUSE

[redacted]

13. [redacted]

14. [redacted]

[redacted]

15. I checked the address 4072 11th Avenue, Sacramento, CA, using Thomson Reuters CLEAR, an online public and proprietary records database used by law enforcement and government agencies to verify names and addresses. No one with the name of [redacted] was associated with the address, however, the most current residents appeared to be "Jose Porras" and "Pasia Vue."

16. I viewed the criminal history records for both PORRAS and VUE, and observed that PORRAS had felony convictions for possessing a firearm and the possession or sales of controlled substances. I then drove by 4072 11th Avenue, Sacramento, and noted the license plate of a Black Mercedes-Benz S550 (the "SUBJECT VEHICLE") parked in front of the residence. The SUBJECT VEHICLE's license plate, California 7ZIV981, returned to Jose PORRAS of 4072 11th Avenue, Sacramento.

17. I then searched the social media website Facebook for profiles of PORRAS and VUE, and located two profiles for VUE. In one Facebook profile for VUE, VUE can be seen in a photograph standing next to a Hispanic male who looks identical to the California Department of Motor Vehicles ("DMV") Driver License photo for PORRAS. I then reviewed the DMV Driver License record for VUE and noted that her address was listed as 4072 11th Avenue, Sacramento, as well. From the above facts I surmised that PORRAS and VUE were possibly dating.

B. CANNA_BARS on the Dream and Hansa dark web marketplaces

18. [redacted] On the Dream Marketplace, I located a vendor using the identity canna_bars ("CANNA_BARS.") CANNA_BARS registered their account on the Dream Marketplace on July 20, 2017, and offered various quantities of "og kush" marijuana for sale.

19. I viewed the Pretty Good Privacy ("PGP")[1] key associated with the account (Fingerprint: 08AC 6416 2ECC 327D AB0C C067 FA3B FD42 6742 30D0) and noted that the PGP key was created on April 5, 2017. As of May 13, 2018, on the Dream Marketplace, CANNA_BARS has 90 reviews from customers, a rating of 4.86 out of 5 stars, and has earned just over $69,000 US Dollars in narcotics sales. Dream Marketplace, like its predecessor dark-web marketplaces, such as Silk Road and AlphaBay, allows vendors to be reviewed by customers and to have a publicly available rating.

20. While reviewing the CANNA_BARS Dream account, I observed that the account had a verified rating from the Hansa marketplace. The Hansa marketplace was taken over by the Dutch National Police ("DNP") for approximately one month in June of 2017 after the arrest of its administrators. While under DNP control, the account details and communications of those who used Hansa were recorded and are now available for law enforcement review.

21. On February 28, 2018, I sent a request to HSI The Hague, Netherlands, and asked for any captured Hansa data for the monikers cannabars and CANNA_BARS. On March 16, 2018, I received the requested data from HSI The Hague. I reviewed this data and observed that CANNA_BARS was also a vendor on Hansa. On Hansa, CANNA_BARS registered his/her

[1] 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.

account on March 24, 2017. In addition to marijuana, CANNA_BARS offered crystal methamphetamine in one-pound quantities, Xanax (Alprazolam) pills, and Promethazine-Codeine cough syrup. Further review of the captured Hansa data revealed that CANNA_BARS earned approximately 56 Bitcoin ("BTC")[2] while operating as a vendor on Hansa, and had approximately 132 positive ratings from customers.

22. On the crystal methamphetamine listing from CANNA_BARS on Hansa, the associated description reads: "this crystal is directly from manufacturers in mexico so it is made with the highest qaulity products that cant be found in the us. expect the highest qaulity on hansa for the cheapest[.]" The unique misspelling of the word "quality" is also found misspelled on CANNA_BARS' Dream Marketplace account, as observed in the message to prospective Dream customers that reads: "whats up we are canna_bars a vendor of top qaulity weed we offer qps to multiple pounds we are operating out of northern california and have direct relationships with many growers so expect good qaulity for cheap prices."

C. Discovery of PORRAS' fingerprints in image posted online by CANNA_BARS

23. While further reviewing the captured Hansa data for CANNA_BARS, I discovered that on June 21, 2017, in response to a request for more pictures of his marijuana offerings, CANNA_BARS posted an album of images to the photo hosting website "Imgur.com." The album posted by CANNA_BARS is located at http://imgur.com/a/uy7PY, and in one photo an open palm holding marijuana buds is displayed. The fingerprints of the open palm are very clear and visible in the photograph.

[2] On May 20, 2018, one Bitcoin is equal to approximately $8,500 USD.

Photo 1 – Image posted by CANNA_BARS to Hansa

24. On March 19, 2018, I downloaded the highest resolution photograph available from the aforementioned album on the Imgur.com website and submitted the photo to the HSI Forensic Document Laboratory ("FDL") for comparison with the known fingerprints of PORRAS captured from his previous arrests. On March 20, 2018, the HSI FDL replied to my latent fingerprint examination request and, in report #18-01630, stated that the visible fingerprints in the photo returned a match to the known fingerprints of PORRAS. The fingerprint identifications were established by a comparative analysis of the friction ridge detail for the fingerprint impressions in question.

D. Marijuana sample ordered from CANNA_BARS on Dream

25. On March 18, 2018, I observed that on his/her Dream Marketplace profile, CANNA_BARS offered a free sample of his "og kush" marijuana to prospective buyers. I then placed an undercover purchase of this free sample, and in a PGP encrypted message, requested that the sample of marijuana be sent to an undercover PO Box in another State. On March 19, 2018, CANNA_BARS sent a tracking number for this parcel. I checked the tracking for this

parcel and observed that it was accepted for shipping at a USPS facility in Sacramento, California.

26. On March 24, 2018, a United States Postal Inspection Service ("USPIS") Inspector and I opened the parcel sent by CANNA_BARS. The parcel, a USPS Priority Mail small-sized box, bore a pre-printed postage label with the sender information of "ADRIAN MORENO 6151 FORDHAM WAY SACRAMENTO CA 95831," and the bogus recipient address provided by HSI to CANNA_BARS. Inside the parcel was a small-sized Duck brand manila envelope wrapped in bubble wrap. Inside the manila envelope was a black Shield-N-Seal vacuum-sealed package. Inside the black vacuum-sealed package was a fabric softener sheet and another clear, vacuum-sealed package. Inside the clear vacuum-sealed package was the free sample of marijuana HSI ordered from CANNA_BARS.

E. PORRAS and VUE liquidate Bitcoin through digital currency exchange

27. On March 26, 2018, I received the results of a subpoena served on a digital currency exchange for accounts matching the known identifiers of PORRAS and VUE. The records returned four accounts created in VUE's name and one in PORRAS' name. In one account created by VUE on April 7, 2017 with the email address "pasiavue57@gmail.com" and telephone number (916) 228-1506, there are several bank accounts attached. Two linked bank accounts are in the name of VUE, a third in the name of Julie Hernandez, and a fourth in the name of Marcos Escobado. Marcos Escobado appears to be a brother or other relative of PORRAS, and has a February 2018 arrest in Oregon for the possession of methamphetamine. In this account, between April 7 and April 15, 2017, just over $11,000 equivalent of BTC was received in four transactions and sold to the digital currency exchange, at which point the fiat currency was sent via ACH transfer to a connected bank account.

F. [redacted]

28. [redacted]

G. THEFASTPLUG located on Wall Street Market dark web marketplace

29. On the Wall Street Market ("WSM,") another dark web narcotics hidden service, a vendor going by the name THEFASTPLUG appears to have the same characteristics as CANNA_BARS' profiles on Hansa and the Dream Marketplace. On WSM, THEFASTPLUG is a registered user since February 2018, and as of May 13, 2018, has 60 completed orders, with a 4.9 out of 5 stars rating. THEFASTPLUG offers "og kush" marijuana and Xanax (Alprazolam) pills for sale, and notably, the blanket in the background of THEFASTPLUG's Xanax photograph is the same red blanket in a photo CANNA_BARS posted to the Hansa market. Additionally, in THEFASTPLUG's WSM profile, the introduction message also misspells the word "quality" as "qaulity" several times. All other information is nearly identical to CANNA_BARS.

[redacted]

30. [redacted]

[redacted]

I. [redacted]

31. [redacted]

32. On April 17, 2018, I conducted an early morning drive-by of the SUBJECT PREMISES and observed PORRAS' 2013 Black Mercedes-Benz S550 (SUBJECT VEHICLE), unoccupied, in the driveway of the residence. [redacted]

33. At approximately 1128 hours I observed PORRAS and VUE in the SUBJECT VEHICLE leaving O'Donnell Avenue. I established mobile surveillance on the SUBJECT VEHICLE and followed it to Interstate 80 westbound, at which point I terminated surveillance. A later review of Public Storage facility records indicates that on April 17, 2018, at approximately 1139 hours, PORRAS' unique gate code was used to enter into the closed, gated area of the storage facility where PORRAS' storage unit (STORAGE UNIT) is located.

34. On April 18, 2018, I requested the customer information for the SUBJECT PREMISES from the Sacramento Municipal Utility District ("SMUD"). Later that day, SMUD replied to my request and provided the customer information that indicates the paying customer for the SUBJECT PREMISES is "PASRA VU." This is the same spelling of PASIA VUE that was on the SMUD records for 4072 11th Avenue, Sacramento - the former residence of PORRAS and VUE.

[redacted]

35. [redacted]

36. [redacted]

37. At approximately 1030 hours, PORRAS was observed leaving his residence in the SUBJECT VEHICLE, at which time law enforcement established mobile surveillance, until losing sight of the SUBJECT VEHICLE near the intersection of Northgate Boulevard and San Juan Avenue. A later review of Public Storage facility records indicates that on May 1, 2018, at approximately 1039 hours, PORRAS' unique gate code was used to enter into the closed, gated area of the storage facility where the STORAGE UNIT is located.

K. Undercover purchase of two pounds of marijuana

38. On May 5, 2018, a USPIS Inspector and I placed an undercover purchase for two pounds of "Double Og Kush" marijuana from CANNA_BARS on the Dream Marketplace. With the order, I sent a PGP encrypted message requesting the parcel be sent to an undercover PO Box controlled by USPIS in another State.

39. On May 7, 2018, law enforcement established surveillance around the SUBJECT PREMISES after confirming that the SUBJECT VEHICLE was at the residence. At approximately 1038 hours, law enforcement observed PORRAS and VUE leaving in the SUBJECT VEHICLE at which time mobile surveillance was established. Law enforcement followed the SUBJECT VEHICLE to the STORAGE UNIT where PORRAS and VUE remained for approximately 10 minutes.

40. From the STORAGE UNIT, law enforcement followed PORRAS and VUE to a U.S. Post Office located at 4401 Gateway Park Boulevard, Sacramento. PORRAS entered the Post Office and returned to the SUBJECT VEHICLE less than 10 minutes later carrying several empty USPS shipping boxes. From the Post Office, law enforcement followed PORRAS and VUE to the Bank of America branch located at or about 1540 West El Camino, Sacramento, at which time VUE exited the SUBJECT VEHICLE and entered the Bank of America property.

41. At approximately 1138 hours VUE exited the Bank of America branch and returned to the passenger seat of the SUBJECT VEHICLE. At this point, law enforcement followed PORRAS and VUE to the U.S. Post Office located at 2000 Royal Oaks Drive, Sacramento. Here, PORRAS entered and purchased with cash two large brown USPS shipping boxes and returned to the SUBJECT VEHICLE. Law enforcement established mobile surveillance and followed the SUBJECT VEHICLE back to the STORAGE UNIT at which time PORRAS and VUE entered the gated facility at approximately 1204 hours.

Photo 2 – PORRAS purchases boxes from Post Office

42. After approximately one and a half hours of not observing the SUBJECT VEHICLE leave the STORAGE UNIT, law enforcement entered the Public Storage office and requested to view storage lockers available for rent. While touring the facility, law enforcement observed the SUBJECT VEHICLE pulled halfway inside the STORAGE UNIT (#E196). At approximately 1423 hours, the SUBJECT VEHICLE departed the STORAGE UNIT location and made its way back to the U.S. Post Office located at 2000 Royal Oaks Drive.

43. At the U.S. Post Office, both PORRAS and VUE exited the SUBJECT VEHICLE, looked around to observe their surroundings, and retrieved three parcels from the trunk of the SUBJECT VEHICLE. Both PORRAS and VUE entered the Post Office and dropped off the three parcels at three different locations to be placed in the mail stream for delivery. At this point a waiting USPIS Inspector retrieved the three parcels for inspection. PORRAS and VUE left the post office separately and returned to the SUBJECT VEHICLE and departed the area at approximately 1440 hours. At this time law enforcement terminated surveillance.

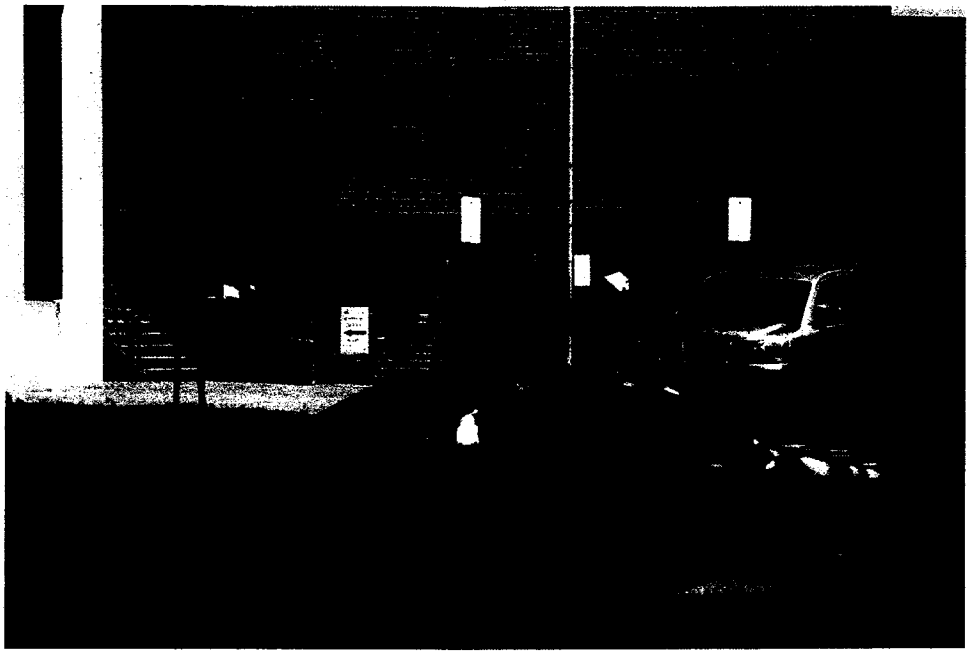


Photo 3 – VUE delivers package to Post Office

44. Law enforcement inspected the three parcels dropped off by PORRAS and VUE and observed that the parcels all bore different return addresses and were destined for locations in Louisiana, Kentucky, and the third parcel was observed to be delivered to the fictitious name and address provided by law enforcement to CANNA_BARS on the Dream Marketplace during the undercover purchase on May 5, 2018. Law enforcement placed the first two parcels back into the mail stream and opened the parcel ordered during the undercover purchase from CANNA_BARS. Inside the parcel were two pounds of marijuana, packaged identical to the free sample of marijuana sent by CANNA_BARS in March 2018, using multiple vacuum-sealed bags, dryer sheets, and Duck brand manila envelopes.

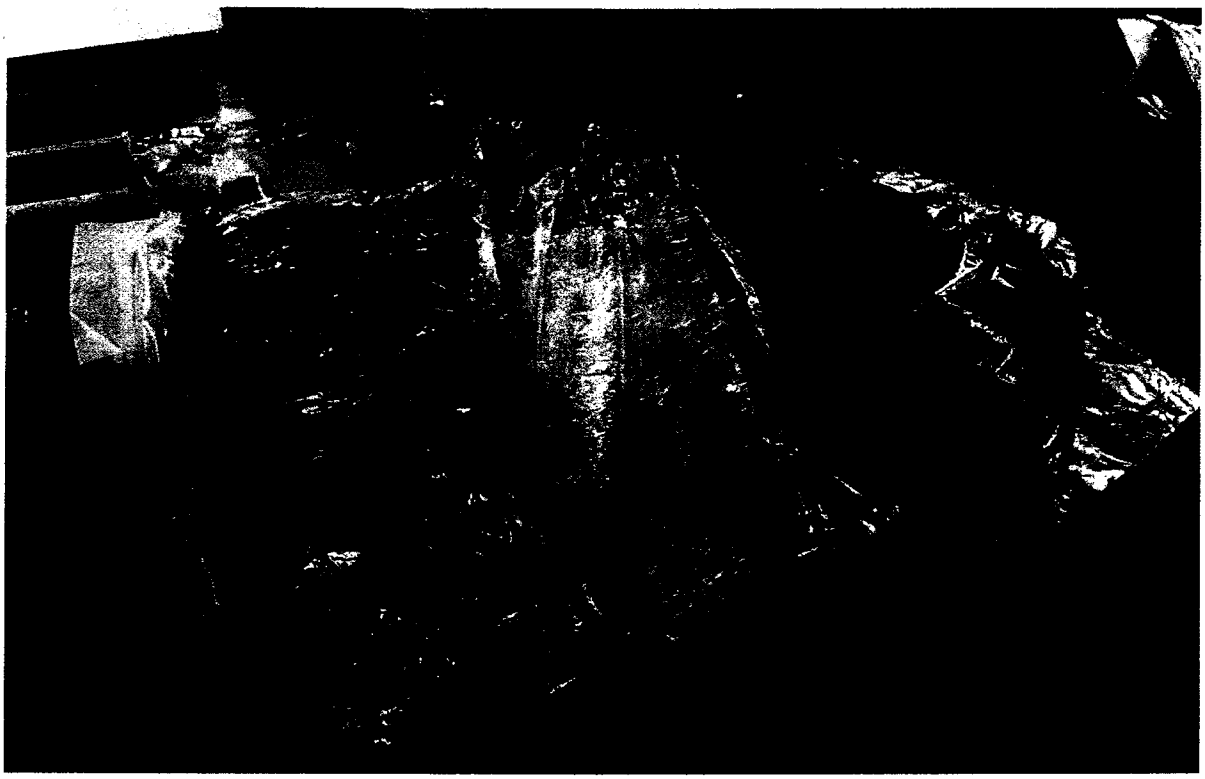


Photo 4 – Marijuana delivered by PORRAS after undercover purchase

[redacted]

45. [redacted]

46. [redacted] At approximately 1119 hours, the SUBJECT VEHICLE turned from O'Donnell Avenue on to Dry Creek Road and made its way to Interstate 80 westbound. At approximately 1127 hours, the SUBJECT VEHICLE arrived at the STORAGE UNIT and then left the storage facility no more than five

minutes later. Law enforcement followed the SUBJECT VEHICLE down Northgate Avenue to El Bramido Mexican Restaurant & Bar, whereupon PORRAS exited the SUBJECT VEHICLE and entered the restaurant. Law enforcement terminated surveillance.

M. Review of Public Storage facility records

47. On May 10, 2018, I served a subpoena on the Public Storage facility located at 3300 Northgate Boulevard, Sacramento, California, where the STORAGE UNIT is located, for records pertaining to the unit in which the SUBJECT VEHICLE was parked halfway inside of during surveillance. A review of these records indicates that unit #E196 was rented by PORRAS on April 1, 2018 under his name, with VUE listed as an alternate contact. The entry and exit logs reveal that PORRAS' unique gate code is used at least two to three times per day, almost daily, to enter the secure storage facility.

N. Undercover purchase of three pounds of marijuana from THEFASTPLUG

48. On May 17, 2018, HSI agents placed an undercover purchase from THEFASTPLUG on WSM for three pounds of "og kush" marijuana to be sent to a PO Box controlled by USPIS in another State. On May 18, 2018, the parcel was mailed to the undercover PO Box from the Land Park Post Office in Sacramento, and on May 20, 2018, had arrived at a USPS Distribution Center in the destination city where the undercover PO Box is located.

[redacted]

49. [redacted]

VI. SEARCH OF DIGITAL INFORMATION

50. Your affiant is aware that users and vendors of online black markets use a computer to access the dark web where online black markets are located. Your affiant is also aware that individuals must use an electronic device to locate and communicate with bitcoin exchangers and purchase bitcoins. Users have to establish an account on an online black market's website to purchase goods and also establish accounts to initiate initial trades with bitcoin exchangers. Users also must establish electronic wallets to receive and send bitcoins to purchase drugs. 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 such as localbitcoins.com, 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 to online black markets, as well as for electronic wallets, are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. Your affiant believes that these are located in the SUBJECT PREMISES, STORAGE UNIT, SUBJECT VEHICLE, and on the persons of PORRAS and VUE.

51. As described above and in Attachment B, your affiant submits that computers, smart phones, and possibly other storage media will be found within the SUBJECT PREMISES, STORAGE UNIT, SUBJECT VEHICLE, and on the persons of PORRAS and VUE, 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 black-market vendor accounts, online digital currency exchange platform accounts, and the data contained therein. Due to the inherent illicit and anonymous nature of these accounts, and that there is no identified

service provider for these accounts, legitimate, compliant or not, to which legal process may be served; your affiant believes this to be the only manner to recover said evidence.

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 the computer(s) for the 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.

66. 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

67. Finally, your affiant respectfully requests that this Court issue an order restricting, until further order of the Court, this case, to include, the Application and Search Warrant. I believe that restricting these documents are necessary to protect the identity of cooperating individuals, because the items and information to be seized are relevant to an ongoing investigation into a criminal organization, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal Affidavits and Search Warrants via the Internet and disseminate them to others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

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) (Manufacture or Distribution of a Controlled Substance); 21 U.S.C. § 846 (Conspiracy to Manufacture, to Distribute, and to Possess with Intent to Distribute a Controlled Substance); and, 18 U.S.C. § 1956 & 1957 (Laundering of Monetary Instruments) are concealed in the locations identified in Attachment 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 the SUBJECT VEHICLE and the items described in Attachment B.

///

///

///

69. Furthermore, I believe that there is probable cause that JOSE ROBERT PORRAS III and PASIA VUE committed those same crimes, thus supporting the legal basis for the Court to issue an arrest warrant based on a criminal complaint.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

Aron Mann
Special Agent
Homeland Security Investigations

Approved as to form:

/s/ Grant B. Rabenn
Grant Rabenn
Assistant United States Attorney

Sworn and Subscribed to me on May 21, 2018

Hon. Carolyn Delaney
United States Magistrate Judge
Eastern District of California

ATTACHMENT A-1

LOCATION TO BE SEARCHED

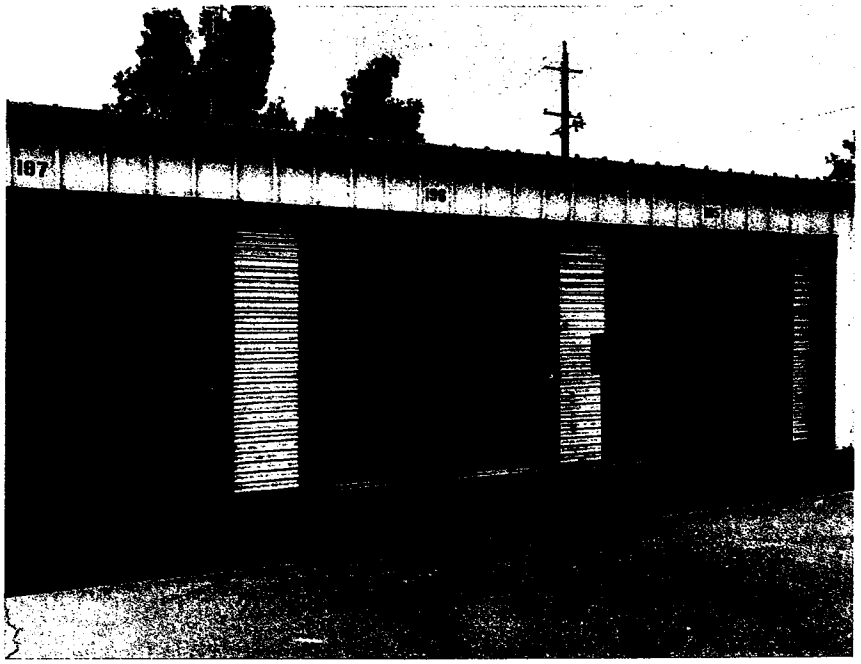
SUBJECT PREMISES – The residence at **1066 O'Donnell Avenue in Sacramento, California 95838** – The property is further described as a single family, one story home in Sacramento, California. The home bears tan siding, a red-brown shingle roof, and a single car garage. The front door is north facing; there is a chain link fence in the front of the property, and the house number 1066 is displayed to the immediate left of the door if looking at the residence.

The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the SUBJECT PREMISES; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at the SUBJECT PREMISES ~~which fall under the dominion and control of the person or persons associated with the SUBJECT PREMISES,~~ and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places or vehicles.

ATTACHMENT A-2

LOCATION TO BE SEARCHED

STORAGE UNIT – The storage unit at **3300 Northgate Boulevard, Unit E196 Sacramento, California 95834** – The property is further described as a 10' x 20' storage unit in the "E" block of buildings, on the ground level in a multi-unit storage facility. The rolling front door is painted orange, is north facing, and has the unit number 196 written directly above the door. A padlock is affixed to the right side of the unit door.

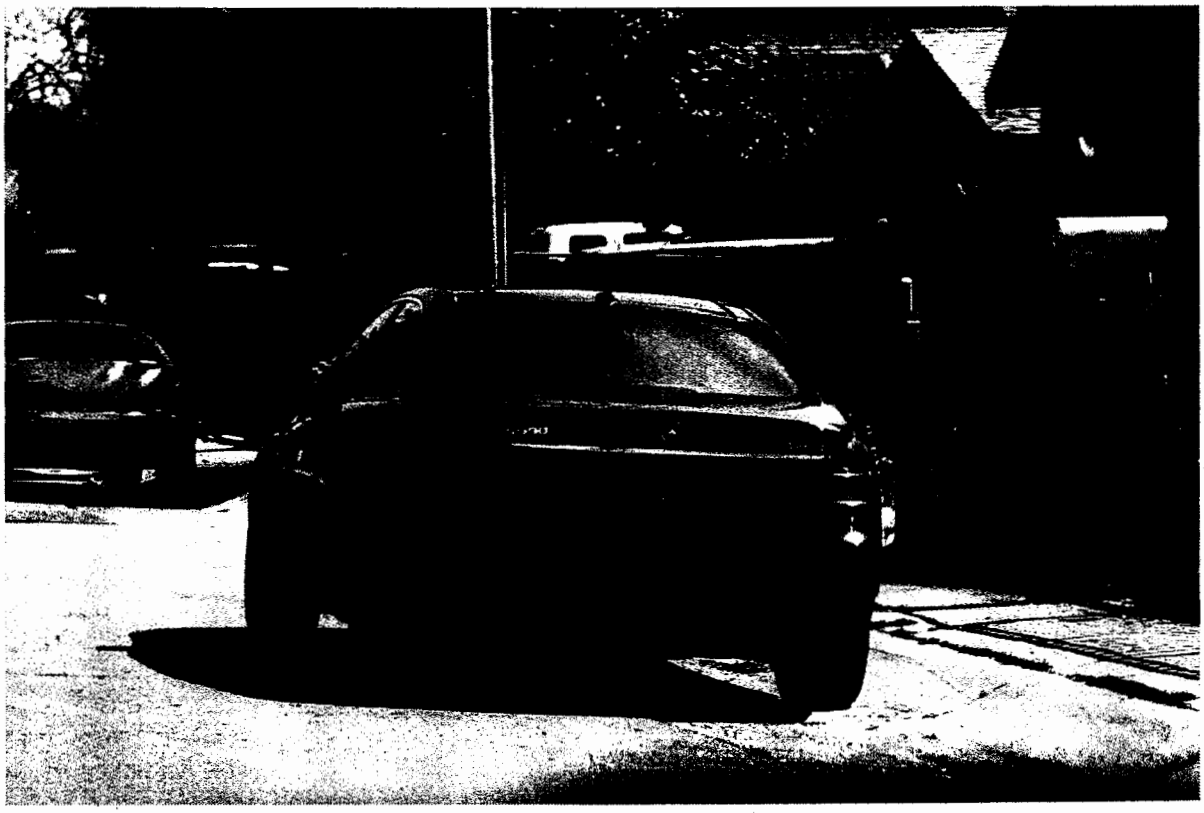


The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the STORAGE UNIT; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at the STORAGE UNIT ~~which fall under the dominion and control of the person or persons associated with the STORAGE UNIT~~; and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places or vehicles.

ATTACHMENT A-3

LOCATION TO BE SEARCHED

SUBJECT VEHICLE – A **2013 Mercedes Benz S550 with license plate 7ZIV981 and VIN WDDNG9EB8DA505449** registered to Jose Robert Porras III at 4072 11th Avenue in Sacramento, California. The Mercedes Benz S550 is black in color and has four doors, with only a rear license plate displayed.



The search of SUBJECT VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained 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) (Manufacture or Distribution of a Controlled Substance); 21 U.S.C. § 846 (Conspiracy to Manufacture, to Distribute, and to Possess with Intent to Distribute a Controlled Substance); and, 18 U.S.C. § 1956 & 1957 (Money Laundering and Conspiracy).

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 SUBJECT PREMISES, STORAGE UNIT, and SUBJECT VEHICLE, 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 PORRAS and VUE, 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 violations 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.

1. Any and all hidden services accounts or encrypted chat applications used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts, Tor-based email accounts, and Wickr handles and logins.

2. 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, including, but not limited to, localbitcoins.com accounts or bitcoin-otc internet relay chat channel accounts.

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 that PORRAS is not legally able to possess or have control over.

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.

2:18-MJ-0102 CKD

/s/ GBR
AUSA INITIALS

PENALTY SLIP

DEFENDANT: Jose Robert Porras III
Pasia Vue

COUNT ONE:

VIOLATION: 21 U.S.C. § 841(a)(1) & (b)(1)(C) - Distribution of a Controlled Substance

PENALTY: 20 years imprisonment
$1,000,000 criminal fine
Mandatory 3 years supervised release

COUNT TWO:

VIOLATION: 21 U.S.C. §§ 846 and 841(a)(1) & (b)(1)(C) - Distribution of a Controlled Substance

PENALTY: 20 years imprisonment
$1,000,000 criminal fine
Mandatory 3 years supervised release

COUNT THREE:

VIOLATION: 18 U.S.C. § 1956 - Money Laundering

PENALTY: 20 years imprisonment
Criminal fine of $500,000 or up to twice the value of the property involved in the transactions, whichever is greater
Up to 3 years supervised release
Forfeiture

COUNT FOUR:

VIOLATION: 18 U.S.C. § 1957 - Money Laundering

PENALTY: 20 years imprisonment
Criminal fine of $500,000 or up to twice the value of the property involved in the transactions, whichever is greater
Up to 3 years supervised release
Forfeiture