AO 91 (Rev. 11/11) Criminal Complaint

REDACTED

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED
MAR 23 2018
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY _____ DEPUTY CLERK

United States of America
v.

CODY MICHAEL WILLIAMS BOYD

Case No. 2:18-MJ-0069 DB

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 December 7, 2017 through present 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), 846	Manufacture or Distribution of a Controlled Substance and conspiracy

This criminal complaint is based on these facts:

(see attachment)

☒ 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: 3-23-18

Judge's signature

City and state: Sacramento, California

Deborah Barnes, 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. Prior to being a Special Agent with HSI, I was an Intern with HSI in Fresno, California. In my capacity as an HSI Intern in Fresno, California, I participated in and guided several investigations involving the distribution of controlled substances on the dark web.

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:

[redacted] **(hereafter referred to as the SUBJECT PREMISES), further described in Attachment A;**

[redacted] **(hereafter referred to as the ROBERTSON PREMISES), further described in Attachment A;**

the seizure of the items described in Attachment B;

and

a criminal complaint naming CODY MICHAEL WILLIAMS BOYD.

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

III. OVERVIEW

5. During this investigation, Federal Law Enforcement Officers have: observed CODY MICHAEL WILLIAMS BOYD ("BOYD"), [redacted], place dozens of suspected narcotics parcels into the United States Postal Service ("USPS") mail system; executed four federal search warrants on parcels containing controlled substances sent by BOYD; executed a federal search warrant on three parcels addressed to BOYD containing the proceeds of narcotics; observed BOYD using a leased business unit to store narcotics parcels; intercepted a parcel from China addressed to BOYD that contained a controlled substance; and, conducted an undercover purchase of cocaine from BOYD. In doing so, BOYD is:

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."

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

A. Initial tip to HSI Sacramento

13. On Thursday, December 7, 2017, HSI Sacramento, California, received a tip from [redacted] that an individual in the Sacramento region was possibly a dark web narcotics vendor. [redacted]

14. I researched the name and learned that an individual with the name Cody Michael Williams BOYD [redacted] once lived in [redacted], however, according to public records, now lives at SUBJECT PREMISES ([redacted]. I then located a Cody Williams BOYD on the social media

website Facebook and noted that most of BOYD's friends who commented on his photographs were from the greater Sacramento area. According to photos posted on BOYD's Facebook profile, BOYD is currently dating a female named Lisa Yang.

15. I then researched the dark web narcotics vendor [redacted] The [redacted] is a dark web online bazaar, similar to the Silk Road. Its customers can purchase narcotics, fraudulent documents, and many other illicit items. These dark web marketplaces can only be accessed by using the TOR (The Onion Router) web browser, and the goods are purchased using digital currencies, predominantly Bitcoin.

16. [redacted]

17. I noted that, on two occasions, posts by [redacted] on his/her [redacted] vendor profile matched up with publicly-available information and photographs posted on BOYD's Facebook profile. [redacted] Based on this information, I began daily surveillance on the SUBJECT PREMISES.

B. **Surveillance of BOYD**

18. Through daily surveillance conducted on SUBJECT PREMISES, I identified a 2011 Black Kawasaki motorcycle (California license plate 20X0396) registered to BOYD, a 2017

White Honda sedan (California license plate 7WAS772) registered to Lisa Yang, and a 2016 Grey Honda Civic ("THE CIVIC") (California license plate 7WCL470) registered to BOYD, all parked in parking space 96 in front of the SUBJECT PREMISES over the course of the week.

19. On Friday, December 15, 2017, law enforcement conducted early morning surveillance at the SUBJECT PREMISES and observed THE CIVIC parked in space 96. At about 11:10 a.m. that day, I also conducted surveillance and saw THE CIVIC, unoccupied, in space 96. Less than 30 minutes later, I saw THE CIVIC leaving the property. I followed it to the United States Post Office located at 2000 Royal Oaks Drive, Sacramento, California. I observed a white male exit the driver's seat and walk across the street into the post office. Based on a review of social media accounts and a Department of Motor Vehicles photo, I concluded that this male was BOYD. Moments later, BOYD returned from the Post Office with two empty USPS mail bins. He placed one in the rear seat of THE CIVIC and loaded the other bin with mail parcels. BOYD then returned inside the post office with one mail bin, dropped nine pre-labeled parcels off at the counter, and left the post office. Law enforcement retrieved the parcels dropped off by BOYD.

Photo 1 – BOYD shipping parcels in the Civic

20. Of the nine parcels dropped off by BOYD at the Royal Oaks Post Office, one was detained for further investigation. Following a positive alert on the parcel by a narcotics detection canine, I secured a federal search warrant (2:17-SW-1091-DB) issued by this Court to search the parcel.

C. [redacted] discovered inside parcel dropped off by BOYD

21. On December 19, 2017, a United States Postal Inspection Service ("USPIS") Task Force Officer ("TFO") and I executed the search warrant on the detained parcel. Inside the seized parcel dropped off by BOYD, the TFO and I discovered approximately [redacted] This parcel was addressed to an individual in the [redacted] and labeled with a bogus return address in San Francisco.

D. BOYD linked to [redacted] through digital currency exchange

22. On December 18, 2017, I received the results of a subpoena served on a digital currency exchange at which BOYD is an account holder. The digital currency exchange identified two accounts for BOYD; the first of which has the username of [redacted] the email of [redacted] and a California driver license registered to [redacted]. Additionally, the name [redacted] was located in the subpoena return. I then located a social media account on the website Instagram, wherein a user going by the name [redacted]

23. The second account located by the digital currency exchange returned the username of [redacted] the email of [redacted] and the telephone number of [redacted]. Later, in January 2018, I called this number from a disposable telephone number and asked for a random male's name, to which the other party replied that I had the wrong number and stated "This is Cody."

E. BOYD purchases 2016 Shelby GT350

24. On December 26, 2017, BOYD posted a photo to his Snapchat account displaying several bundles of US currency, with the appended caption of [redacted] On January 2, 2018, I conducted surveillance at the SUBJECT PREMISES and observed a black [redacted] bearing a temporary CarMax license plate parked in space 96.

25. I later learned that on December 26, 2017, BOYD purchased a cashier's check at Wells Fargo with $40,000 in cash, and put that check toward the purchase of the [redacted] at CarMax. On the credit application for the [redacted], BOYD indicated that he was self-employed, that his business name was [redacted] and that his monthly gross income was $7,292.00.

F. Intercept of package containing [redacted] addressed to SUBJECT PREMISES

26. On January 4, 2018, I was notified by officers from the U.S. Customs and Border Protection ("CBP") that an international mail parcel from [redacted], was destined for Cody BOYD at the SUBJECT PREMISES. The parcel was identified by CBP as being shipped from a known narcotics violator. I requested that the incoming parcel be detained and inspected for any contraband. The parcel was detained at a CBP facility, and an enforcement exam revealed [redacted]. The [redacted] was sent to a CBP scientific services lab for analysis.

27. On January 19, 2018, I learned that [redacted] tested positive for [redacted]

G. BOYD mails [redacted] parcel using [redacted] vehicle

28. On January 8, 2018, law enforcement conducted surveillance at the SUBJECT PREMISES and observed the [redacted] parked in space 96. During the surveillance, BOYD

walked out of the SUBJECT PREMISES carrying a large number of USPS parcels. BOYD made multiple trips from the residence to the [redacted], placing numerous USPS parcels in the trunk of the vehicle.

29. Mobile surveillance was established on the [redacted] as it departed the residence. Law enforcement followed BOYD until he parked in the parking lot of the United States Post Office, located at 2000 Royal Oaks Drive, Sacramento, California. BOYD retrieved the parcels from the trunk of the [redacted] and made two trips into the post office dropping the pre-labeled parcels off at the counter. Law enforcement immediately took custody of the 24 parcels mailed by BOYD. Following the mailing of the parcels, law enforcement observed BOYD retrieve mail from [redacted], which is located in the Post Office lobby. Law enforcement reviewed the application on file for the person renting [redacted] and noted the box was registered to BOYD and listed the SUBJECT PREMISES as his address. One of the 24 parcels mailed by BOYD was detained for further investigation.

30. A federal search warrant for the parcel was issued by this Court (2:18-SW-0017-KJN). As a result of the search warrant, law enforcement seized [redacted]

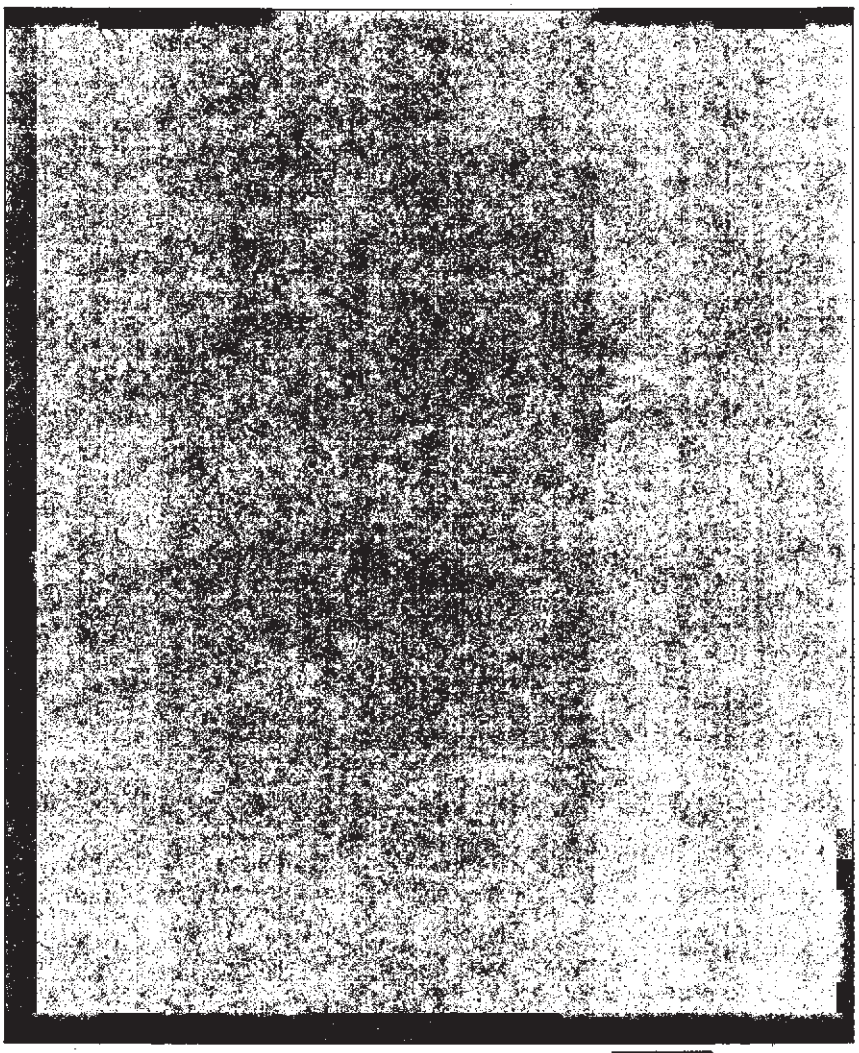


Photo 2 – BOYD shipping parcels in the [redacted]

H. BOYD receives cash in mail

31. On February 8, 2018, while conducting surveillance, law enforcement observed a silver Ford F-150 bearing dealer plates and the words "PARAMOUNT SPEED" written on the rear window, parked in space 96 at the SUBJECT PREMISES. I know from observing BOYD's social media accounts that on February 4, 2018, BOYD dropped his [redacted] off at a vehicle tuning shop named Paramount Speed in Chico, California, to receive an engine upgrade.

32. During this surveillance, law enforcement observed BOYD leave the SUBJECT PREMISES and enter the Ford F-150. Mobile surveillance was established, and law enforcement followed BOYD to the Royal Oaks Post Office. Earlier in the day, a USPIS

Inspector checked BOYD's PO Box at the Royal Oaks Post Office and observed and photographed six parcels delivered to the box, all of which appeared to be consistent with parcels containing bundles of cash.

33. BOYD entered the Post Office, removed the suspected money parcels from the PO Box, and walked back to the F-150. Law enforcement maintained surveillance on BOYD while he remained sitting in the F-150 in the Post Office parking lot and proceeded to open up each of the parcels that he just retrieved from his PO Box. Law enforcement observed as BOYD removed unknown amounts of currency from the six parcels and counted it, while sitting in the F-150 in the parking lot.

34. On February 9, 2018, during surveillance on the SUBJECT PREMISES, I observed and photographed BOYD leave his apartment and discard into a trash bin the packaging from the six parcels he retrieved and opened in the F-150 the previous day.

35. On February 13, 2018, a USPIS Inspector observed numerous parcels were to be delivered again to BOYD's PO Box. The Inspector detained three of the parcels, all consistent with containing narcotics proceeds, and secured Federal search warrants for the parcels, issued by this Court (2:18-SW-129-EFB; 2:18-SW-130-EFB; and, 2:18-SW-131-EFB).

36. On February 14, 2018, the Inspector executed the search warrants on the three detained parcels. Each of the three parcels contained different amounts of US Currency concealed in them, ranging from $355.00 to $1,560.00. After surreptitiously opening the parcels and documenting the process with photographs, the contents were placed back in the parcels and sealed to their nearly original state. The Inspector placed the parcels back in BOYD's PO Box, and BOYD retrieved them later that afternoon.

37. While monitoring BOYD's PO Box, law enforcement discovered that between approximately December 1, 2017 and February 28, 2018, BOYD received over 90 parcels containing suspected narcotics proceeds. In addition to the suspected money parcels, BOYD also received a large number of international parcels suspected of containing narcotics and/or components of his drug distribution operation. Every parcel delivered to the PO Box observed

by law enforcement was addressed to Cody BOYD. Law enforcement noticed no other "legitimate" mail was ever delivered to the PO Box, indicating the box was likely opened for the sole purpose of avoiding detection from law enforcement and facilitating his narcotics distribution operation.

I. BOYD opens new PO Box

38. On February 20, 2018, BOYD opened a new PO Box, [redacted], at the Post Office located at 2121 Broadway, Sacramento, CA. On the PO Box application, BOYD listed his address as the SUBJECT PREMISES, the email of [redacted] and the business name of [redacted]

J. Undercover purchase of [redacted] from BOYD

39. On February 6, 2018, a USPIS Inspector and I purchased [redacted] from BOYD's dark web vendor store on the [redacted]. Before purchasing [redacted], I sent a message to BOYD's dark web persona, [redacted], and inquired if his [redacted] was in stock and available for purchase. BOYD, [redacted], replied "Well do 1oz and see how u like it if you like it Iv got tons." The [redacted] was purchased for approximately [redacted]. With the order, I sent a Pretty Good Privacy ("PGP") encrypted message to BOYD instructing him to deliver the [redacted] to an undercover PO Box in control of the USPIS. The PGP key given by [redacted] on the [redacted] has the email [redacted] associated with it.

40. On February 26, 2018, the USPIS Inspector received the parcel containing the [redacted] purchased from BOYD. The [redacted] inside the parcel was field tested using a Scott Reagent System designed to test [redacted], to which the test returned an immediate positive result. [redacted]

K. Discovery of ROBERTSON PREMISES

41. On March 9, 2018, law enforcement conducted surveillance at the SUBJECT PREMISES and observed BOYD leave in the [redacted] now covered in a white "wrap" bearing BOYD's other [redacted] This instance was peculiar in that BOYD did not carry any parcels out of the SUBJECT PREMISES into his vehicle. Law enforcement established mobile surveillance on BOYD and followed him on a new route, but shortly lost sight of him. Approximately an hour after losing sight of BOYD, BOYD arrived at the Royal Oaks Post Office in the [redacted] and mailed a handful of suspected narcotics parcels.

42. On March 12, 2018, law enforcement established surveillance at the SUBJECT PREMISES and followed BOYD on this new route again, to a business complex located at the ROBERTSON PREMISES. BOYD entered the business suite and returned approximately 15 minutes later with a handful of USPS parcels. BOYD returned to the door of the ROBERTSON PREMISES and locked it shut with a key on his keyring. Law enforcement followed BOYD to the Royal Oaks Post Office where BOYD mailed approximately eight parcels, each of which bore a return sender name of either [redacted] or [redacted]

43. Upon inspecting the parcels dropped off by BOYD, law enforcement recognized one of the recipient names as someone who has received parcels from BOYD in the past, as well as sent suspected money parcels to BOYD's PO Box. Law enforcement seized one of the two parcels destined for this individual and secured a Federal search warrant from this Court (2:18-SW-0206-DB) to search its contents. On March 22, 2018, a USPIS Inspector executed the search warrant and discovered approximately [redacted] in the detained parcel that originated from the ROBERTSON PREMISES.

44. I recognized the ROBERTSON PREMISES from two Snapchat videos posted by BOYD on February 6 and February 13, 2018. In these videos, BOYD is recording from the inside of the business and setting an alarm code in one video, and letting his dog run around inside suite in the second video. The exterior parking lot can be seen in this video, and it is identical to the exterior

of the ROBERTSON PREMISES. Additionally, a light colored Toyota can be seen parked outside in one of the videos, and this vehicle is parked outside of the ROBERTSON PREMISES in the Google Maps photo of the business suite as well.

45. On March 13, 2018, law enforcement established surveillance at the SUBJECT PREMISES and observed as BOYD arrived at the ROBERTSON PREMISES once again. BOYD unlocked the door to the business suite, entered, and returned shortly later with a large box of USPS parcels in tow. Law enforcement observed BOYD lock the door to the ROBERTSON PREMISES business suite and drive to the Royal Oaks Post Office, where BOYD mailed approximately 17 suspected narcotics parcels, each of them bearing the return sender name of either [redacted] or [redacted]

VI. SEARCH OF DIGITAL INFORMATION

46. Your affiant is aware that users and vendors of online black markets use a computer to access the Deep 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, ROBERTSON PREMISES, SUBJECT VEHICLE, and on the person of BOYD.

47. 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, ROBERTSON PREMISES, SUBJECT VEHICLE, and on the person of BOYD, 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. "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.

56. 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.

57. 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:

58. 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.

59. 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.

60. 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.

61. 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.

62. 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

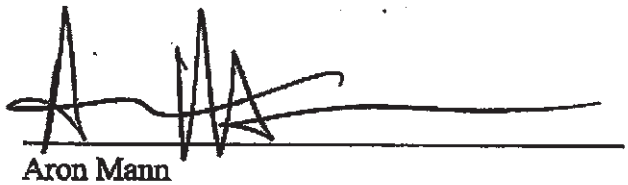
63. Finally, your affiant respectfully requests that this Court issue an order restricting, until further order of the Court, this case, to include, the Application and Search Warrant. I believe that restricting these documents are necessary to protect the identity of cooperating individuals, because 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

64. 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) are concealed in the locations identified in Attachments A-1 through A-3. Accordingly, I respectfully request the issuance of a search warrant authorizing the search of the locations described in Attachments A-1 through A-3, as well as the seizure of the items described in Attachment B.

65. Furthermore, I believe that there is probable cause that CODY MICHAEL WILLIAMS BOYD 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:

Paul Hemesath
Assistant United States Attorney

Sworn and Subscribed to me on March 23, 2018

Hon. Deborah Barnes
United States Magistrate Judge
Eastern District of California

ATTACHMENT A-1

LOCATION TO BE SEARCHED

SUBJECT PREMISES – The residence at [redacted] - The property is further described as a single family apartment on the ground level in a multi-unit apartment building. The front door is west facing with a staircase directly in front of its opening, and has the unit number 774 to the immediate left of the door. The apartment building has beige siding. There is a small, enclosed patio to the side of the front door, with a sliding glass door leading into the apartment.

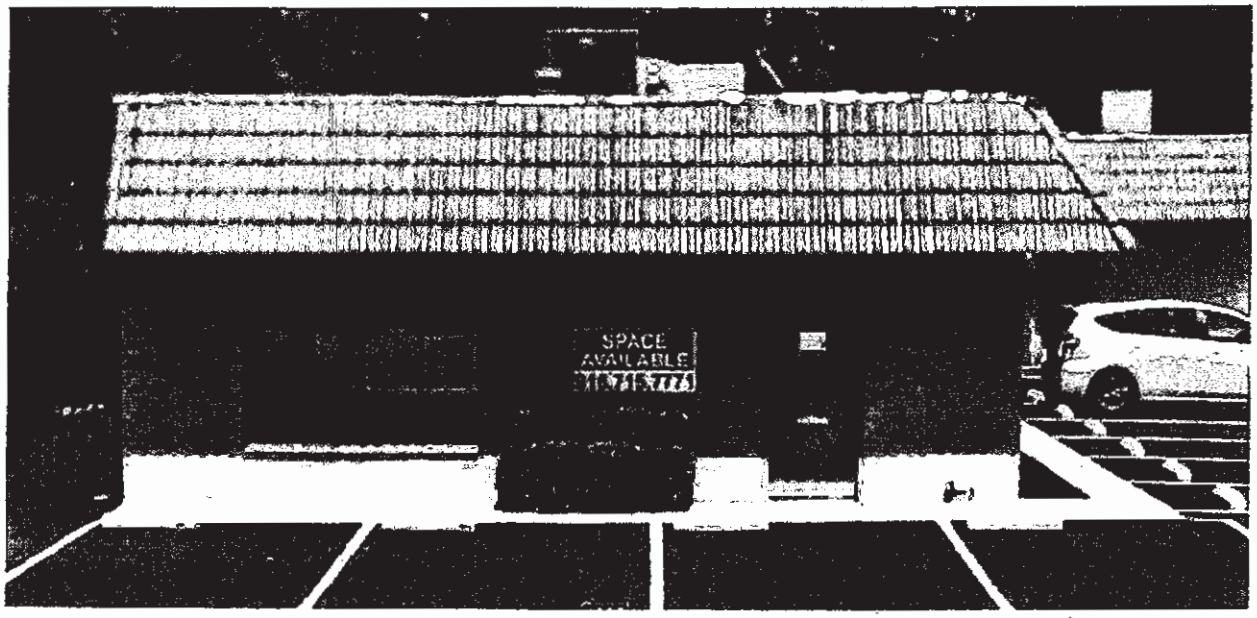
The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the SUBJECT PREMISES; any computer, digital devices, and digital media located therein, where the 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

ROBERTSON PREMISES – The premises of [redacted] – The property is further described as a two suite business unit with a peach brick exterior and a red roof. One door, facing south, allows entrance to the business suite. On the south and east sides of the suite are located a panel of windows giving view into the suite.

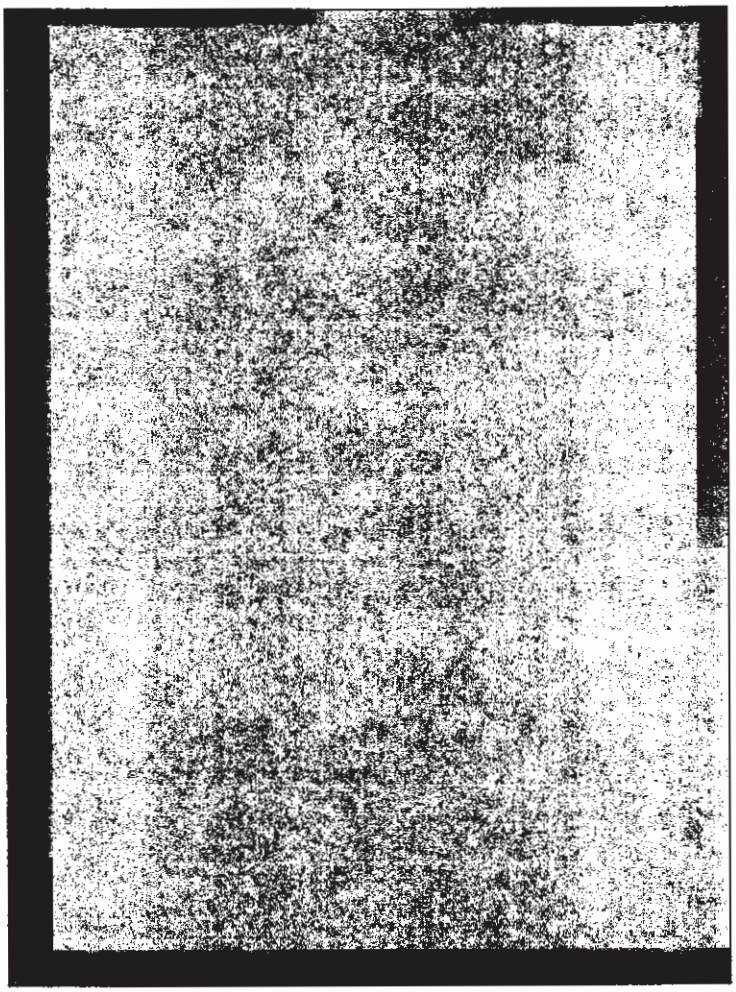


The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the ROBERTSON PREMISES; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at the ROBERTSON PREMISES which fall under the dominion and control of the person or persons associated with the ROBERTSON 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-3

LOCATION TO BE SEARCHED

SUBJECT VEHICLE – A [redacted] with license plate [redacted] and VIN [redacted] registered to Cody Michael Williams at [redacted] The [redacted] is black in color, but bears a white-colored "wrap" displaying BOYD's [redacted]



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 aforementioned 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):

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 found in the Subject Premises, 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, 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 BOYD, 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. 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.

WITH REGARD TO DATA AND DEVICES CLEARLY PERTAINING TO PERSONS OTHER THAN CODY MICHAEL WILLIAMS BOYD, EXAMINING AGENTS SHALL MAKE EFFORTS TO (1) RETURN DEVICES THAT BELONG TO OTHER PERSONS, AND (2) SEGREGATE SUCH DATA FROM FURTHER EXAMINATION BY MEANS OF FLAGGING KEYWORDS OR OTHER REASONABLE METHODS. IF AGENTS FIND EVIDENCE OF CRIMES COMMITTED BY OTHER PERSONS IN PLAIN VIEW, AGENTS SHALL APPLY FOR AN ADDITIONAL WARRANT TO SEIZE SUCH DATA.