AO 91 (Rev. 11/11) Criminal Complaint

Sealed

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Matthew Jones, a/k/a "CALIGIRL," a/k/a "Dynamite2k," a/k/a "Dynamite`," a/k/a "Tyler Zeddai," a/k/a "Mateo Jones"

Defendant(s)

Case No. 6:14-mj- 1233

CRIMINAL COMPLAINT

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

On or about the date(s) of July 11, 2013 - March 20, 2014 in the county of Seminole in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1) and 841(b)(1)(C)	Distribution of a controlled substance (Oxycodone)

I certify the foregoing to be a true and correct copy of the original.
[illegible]
United States District Court
Middle District of Florida
By: [signature]
Deputy Clerk

This criminal complaint is based on these facts:

See attached affidavit

☑ Continued on the attached sheet.

Complainant's signature

Jared Gabbay, DEA Task Force Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/14/14

Judge's signature

City and state: Orlando, FL

Gregory J. Kelly, U.S. Magistrate Judge
Printed name and title

State of Florida
County of Orange

6:14-mj- 1233

AFFIDAVIT

I, Jared Gabbay, being duly sworn, state as follows:

Introduction

1. I am a Task Force Agent (TFA) with the Drug Enforcement Administration (DEA) Miami Field Division where I am currently assigned to the DEA Orlando District Office Tactical Diversion Squad (TDS). The TDS is composed of DEA Special Agents (SA), DEA Diversion Investigators (DI), and deputized TFAs charged with investigating drug trafficking and money laundering offenses specifically related to the diversion of pharmaceutical controlled substances. I have been employed as a TFA with DEA since March 2013. As a TFA, my duties include the investigation of violations of federal controlled substances laws and other criminal violations related to the illegal distribution of controlled substances, including violations of federal money laundering laws.

2. I have been employed as a full time law enforcement officer for approximately 10 years. Since 2005, I have been employed by the Orange County Sheriff's Office (OCSO). Prior to joining OCSO, I was employed by the City of Key West Police Department.

3. I have received training and information regarding the structure and investigation of narcotic crimes and organized criminal organizations from schools, other narcotics investigators, supervisors, and prosecutors, and have

conducted extensive investigations of organized criminal racketeering offenses and narcotics crimes, including the use of visual surveillance, electronic surveillance, informant interviews, interrogations, and undercover operations. In connection with drug trafficking investigations, I have participated in and/or executed numerous search warrants, including those on residences of drug traffickers/manufacturers and their co-conspirators. I have previously been assigned to the Metropolitan Bureau of Investigation (MBI) Vice/Organized Crime squad, the OCSO Street Crimes Unit, and the OCSO Undercover Narcotics Unit. I have additional advanced training and experience in Computer Networking and Unix Systems Administration.

4. The information in this affidavit is based on my personal knowledge of, and participation in, this investigation, information from other criminal investigators and law enforcement officers, financial institutions, other business entities, as well as other documents and records obtained by law enforcement during the course of this investigation.

5. The information set forth herein is provided for the limited purpose of establishing probable cause. Because this affidavit is submitted for the limited purpose of establishing such probable cause, it does not include all of the details of this investigation of which I am aware.

Purpose of this Affidavit

6. This affidavit is submitted in support of a criminal complaint and arrest warrant for Matthew Jones, a/k/a "CALIGIRL," a/k/a "Dynamite2k," a/k/a

"Dynamite`," a/k/a "Tyler Zeddai," a/k/a "Mateo Jones" for violations of 21 U.S.C. §§ 841(a)(1) and 841(b)(1)(C) (distribution of a controlled substance).

Structure of this Affidavit

7. This affidavit is divided into separate sections to present the information herein to the Court. First, I provided "Summary of the Investigation" which gives an overview of the investigation and evidence which is subject of this affidavit. Second, I provided a "Subject of this Investigation" section. Third, I provided a "Background on Silk Road, Bitcoins, and Bitmessage" in which I explain the Silk Road drug marketplace, Bitmessage, and related technical aspects of the investigation. Fourth, I detail the "Probable Cause" that supports the offenses detailed in this affidavit. Within the "Probable Cause" section of the affidavit, I detail a "Background of Silk Road Vendor "CALIGIRL" and describe a "Silk Road sales analysis for CALIGIRL." Furthermore, I detail "Undercover Purchases and Seizures of Controlled Substances" and I describe the "Package Profile" utilized during the investigation. Next, I detail "Mail Drop/Receipt Locations Utilized by Jones" and I describe "Jones' Purchases of Packaging Materials on Amazon.com." In the next section, I detail "Public Domains Associated with Matthew Jones." Next, I explain a "North Texas Tollway Authority Records" analysis, "Jones' International Travel to Colombia," and an "Origin of Oxycodone Products Offered for Sale by CALIGIRL." Lastly, I conduct a "Financial Analysis" of Jones' bank accounts.

Summary of the Investigation

8. This investigation determined that Matthew Jones, using the alias "CALIGIRL," illegally sold controlled substances on the Silk Road drug marketplace website. According to CALIGIRL's Silk Road vendor profile, CALIGIRL was among the top 5% of all vendors operating on the Silk Road.

9. As part of the investigation, I made two (2) undercover purchases from CALIGIRL's Silk Road account and six (6) additional undercover purchases from CALIGIRL outside of the Silk Road website utilizing an encrypted and anonymized program called Bitmessage. CALIGIRL only accepted the crypto-currency Bitcoin as currency for the purchase of controlled substances.

10. The investigation determined that CALIGIRL offered controlled substances for sale that, once purchased, were delivered to customers by the United States Postal Service (USPS). During the course of this investigation, I identified a commercial mailbox in Arlington, Texas that was being used to receive shipments of controlled substances. After Jones received the controlled substances, he then resold and distributed the controlled substances throughout the United States.

11. During the course of the investigation, a shipping package profile of Jones' parcels was developed. This profile was developed from the known packages received from undercover purchases and additional known packages linked to Jones. The dimensions, weights, and packaging of the additional packages identified were consistent with packages sent by Jones that were

seized by law enforcement. Based upon the reliable package profile developed from the known packages being sent through the USPS, more than 100 additional packages were identified as having been mailed by Jones.

12. In addition to the eight (8) undercover controlled substance purchases from Jones/CALIGIRL, an additional four (4) packages containing controlled substances were seized and searched pursuant to federal search warrants issued by the United States District Court in the Northern District of Texas. To date, more than 400 Oxycodone tablets and more than 900 Hydrocodone tablets have been seized or purchased from Jones.

13. An analysis of bank records and business records confirmed that Jones was the person operating the CALIGIRL Silk Road account and that Jones was the person responsible for selling and shipping the controlled substances on Bitmessage.

Subject of this Investigation

14. Matthew Jones, a/k/a "CALIGIRL," a/k/a "Dynamite2k" a/k/a "Dynamite`," a/k/a "Tyler Zeddai," a/k/a "Mateo Jones" was most recently employed as the Chief Technology Officer for Data Paradigm, Inc. Data Paradigm is a business process software consulting firm headquartered in Dallas, Texas.

15. Jones is also listed as the Chief Technology Officer for iTransact, Inc., an online merchant services company.

16. Jones does not possess any lawful authority to possess, import, dispense, prescribe, or otherwise distribute any controlled substance. Jones does not now, nor did he ever, possess a DEA registration number.

17. Jones' current home address is 13625 Far Hills Lane, Dallas, Texas. Jones also maintains a commercial mailbox located at 1861 Brown Boulevard, Box 620, Arlington, Texas. As further detailed in this affidavit, this commercial mailbox is registered under Jones' name and one of Jones' aliases, "Tyler Zeddai."

18. Jones frequently travels to Colombia, a source country for the Oxycodone products he offers for sale.

19. Jones maintained an account on http://localbitcoins.com under the alias of "Dynamite2k" and an account on http://www.bitcoin-otc.com/ under the alias "Dynamite`." These websites are designed for peer-to-peer Bitcoin to national currency "exchanges." An exchange is used to convert a virtual currency into a national currency, or vice versa. Through his use of these websites, Jones exchanged Bitcoins earned from his illegal sales of controlled substances into U.S. dollars.

Background of Silk Road, Bitcoins, and Bitmessage

20. In the course of this investigation, I gained extensive familiarity and knowledge about the Silk Road website. The Silk Road website provided a sales platform that allowed vendors and buyers who were users of the website to conduct transactions online. The basic user interface resembled those of well-

known online marketplaces. However, unlike mainstream e-commerce websites, Silk Road was only accessible on the TOR network. Based on my training, experience, and this investigation, I know that TOR is a special network of computers on the Internet, distributed around the world. The TOR network is designed to conceal the true Internet Protocol (IP) addresses of the computers on the network, and, as a result, the identities of the network's users.[1] Although TOR has legitimate uses, it is also known to be used by criminals seeking to anonymize their illegal online activities. Every communication sent through TOR is routed through numerous relays within the TOR network and is wrapped in numerous layers of encryption, such that it is practically impossible to trace the communication back to its true originating IP address. The encryption is designed to prevent even the TOR relay servers from knowing the true origin and destination of a communication. TOR likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the website. Such "hidden services" operating on the TOR network have complex web addresses, generated by a computer algorithm, ending in ".onion." For example, the address for the Silk Road website was https://silkroadvb5piz3r.onion."[2]

---

[1] Every computer device connected to the Internet has an Internet Protocol or "IP" address assigned to it. The IP address is utilized to route traffic to and from the device. A device's IP address can be used to determine its physical location, internet provider and, thereby, its user.

[2] The Silk Road website was seized on October 2, 2013 by the Federal Bureau of Investigation pursuant to a seizure warrant issued in the United States District Court for the Southern District of New York.

21. Websites with ".onion" addresses are only accessible using the TOR browser software or by utilizing one of several TOR proxy websites, such as https://onion.to. TOR proxy websites allow a user to access TOR services, but do not provide the user the same level of anonymity. The TOR browser software is easily downloaded, at no cost, on the internet.

22. In order to access the Silk Road website, a user needed to only download the TOR browser software onto his/her computer and then type the Silk Road's ".onion" address in to the TOR browser address bar. The Silk Road's ".onion" address could be found by utilizing any Internet search engine and was listed in numerous places on the regular Internet.

23. Upon being directed to the Silk Road website, a user was presented with a black screen containing a prompt for a username and password, as well as a link that said, "Click here to join." No further explanation about the site was given. Based on my training, experience, and this investigation, such cryptic login screens are often used by criminal websites in order to restrict access to users who already know about the illegal activity on the site, typically through word of mouth, in Internet forums, and on Internet Relay Chat networks, and deliberately seek to enter.

24. Upon clicking the link on the Silk Road login screen to join the website, the user was prompted to create a username, password, and identify the country where he/she was located. No other information was requested and the country-location information was not required, nor was it subject to

verification. After entering a username and password, the user was then directed to Silk Road's homepage. At the top left corner of the homepage there was a logo for the website labeled "Silk Road anonymous market." On the left side of the screen there was a list titled "Shop by Category" which contained links to various categories of items for sale on the website. In the center of the screen, there was a collection of photographs that reflected a sample of the current listings on the site. At the top of the screen, there was a link labeled "messages" through which the user could click on to access Silk Road's "private message" system. This system allowed users to send messages to one another through the site, similar to e-mails. At the bottom right of the screen, there was a link labeled "community forums" which led to an online forum where Silk Road users could post messages to "discussion threads" concerning various topics related to the website. This link was identified as the "Silk Road forum." Also at the bottom right of screen, there was a link labeled "wiki," which led to a collection of "frequently asked questions" and other forms of guidance for site users. This link was identified as the "Silk Road wiki." The bottom right of the screen also contained a third link labeled "customer service" which led to a customer support page where users could "open a support ticket" and contact an "administrator" who, the webpage said, "will take care of you personally."

25. Clicking on any of the links to items for sale on the Silk Road website brought up a webpage that contained the details of the listing, including a description of the item, the prices of the item, the user name of the vendor selling

it, and "reviews" of the vendor's "product" posted by previous customers. An example of a listing is attached to this affidavit as Exhibit 1. To buy an item listed for sale, the user could simply click the link on the listing labeled "add to cart." In order to confirm an order, the user was prompted to provide a shipping address. Once the order was placed, it was processed through the Silk Road's Bitcoin based payment system.

Illegal Goods and Services Sold on the Silk Road Website

26. The illegal nature of the items sold on the Silk Road was readily apparent to any user browsing through its inventory. The vast majority of the goods for sale consisted of illegal drugs of nearly every variety, which were openly advertised on the website and prominently visible on the website's home page.

27. As of September 23, 2013, there were nearly 13,000 listings for controlled substances on the website listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others. Clicking on the link for a particular listing brought up a picture and description of the drugs being offered for sale. For example, listings stated "2.5ml THC e juice made from BHO," "10 x 20mg Oxycontin – OC Formula Crush," and "QUALITY #4 HEROIN ALL ROCK."

28. The controlled substances sold on the Silk Road website tended to be sold in individual-use quantities, although some vendors would sell in bulk. The offerings for sale on the website, at any single time, amounted to multi-

kilogram quantities of heroin, cocaine, methamphetamine, methylene, MDMA, Oxycodone, Hydrocodone and various other controlled substances.

29. In addition to illegal narcotics, other illicit goods and services were openly sold on Silk Road. For example, as of September 23, 2013, there were 159 listings on the site under the category "Services" and most concerned computer-hacking services. For example, one listing was by a vendor that offered to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing so that "You can Read, Write, Upload, Delete, View All Personal Info." Another listing offered tutorials on "22 different methods" for hacking Automatic Teller Machines (ATM). There were 801 listings under the category "Digital goods," including offerings for pirated media content, hacked accounts at various online services such as Amazon and Netflix, and listings for malicious software. There were 169 listings under the category "Forgeries," placed by vendors offering to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of identity documents. There were 280 listings under the category "Money," placed by vendors offering to launder currency and exchange Bitcoins for various national currencies. Included in this category were listings for "Cash in the Mail" in exchange for Bitcoins and tutorials on offshore banking and avoiding money laundering laws.

30. Not only were the goods and services offered on the Silk Road overwhelmingly illegal on their face, but the illicit nature of the commerce

conducted through the website was candidly recognized in the Silk Road wiki and the Silk Road forum. For example, the Silk Road wiki contained a "Seller's Guide" and "Buyer's Guide" that contained extensive guidance for users on how to conduct transactions on the website without being caught by law enforcement. The "Seller's Guide" instructed vendors to "vacuum seal" packages that contained controlled substances narcotics, in order to avoid detection by "canine or electronic sniffers." Meanwhile, the "Buyers Guide" instructed buyers to "[u]se a different address" from the user's own address to receive a shipment of any item ordered through the site, "such as a friend's house or P.O. box" from which the user could then "transport [the item] discreetly to its final destination."

31. Likewise, the Silk Road forum contained extensive guidance, posted by users of the site themselves, on how to evade law enforcement. For example, in a section of the forum labeled "Security - Tor, Bitcoin, cryptography, anonymity, security, etc.," there were numerous postings by users that offered advice to other users on how they should configure their computers to avoid leaving any trace on their systems of their activity on Silk Road.

Silk Road's Bitcoin Based Payment System

32. The only form of payment accepted on the Silk Road was Bitcoins. Bitcoins are an anonymous, decentralized form of electronic "currency," existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company. Rather, a Bitcoin is generated and controlled automatically through computer software operating on a "peer-to-peer"

network. Bitcoin transactions are processed collectively by the computers composing the network.

33. To acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments in some conventional form of currency (cash, wire transfer, etc.) and exchange the money for a corresponding number of Bitcoins. Exchangers also accept payments of Bitcoin and exchange the Bitcoins back to conventional currency, again, charging a commission for the service. Bitcoin exchangers are generally not registered with state or federal regulation bodies such as the Financial Crimes Enforcement Network (FinCEN) and many operate as unlicensed money transmitting services. The value of a Bitcoin is based on a fluctuating exchange rate.

34. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in a "wallet" associated with a Bitcoin "address" as designated by a complex string of letters and numbers. The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored. Once a Bitcoin user funds his or her wallet, the user can then use Bitcoins in the wallet to conduct financial transactions by transferring Bitcoins from their Bitcoin address to the Bitcoin address of another user, over the Internet.

35. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system

operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and, therefore, cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin involved in a set of transactions is it possible to meaningfully trace funds through the system.

36. Bitcoins are not illegal in and of themselves and may have legitimate uses. However, Bitcoins are known to be used by criminals for money laundering purposes, given the ease with which they can be used to move money anonymously.

37. Silk Road's payment system consisted of a Bitcoin "bank" internal to the website where every user had to have an account in order to conduct transactions. Specifically, every user on Silk Road had a Silk Road Bitcoin address or had multiple addresses associated with the user's Silk Road account. These addresses were stored on wallets maintained on servers controlled by Silk Road. A user could request a new wallet address at any time.

38. In order to make a purchase on the Silk Road, the user had to first obtain Bitcoins and send them to a Bitcoin address associated with the user's Silk Road account. After funding a user account, the user could then make purchases from Silk Road vendors. When the user purchased an item on Silk Road, the Bitcoins needed for the purchase were held in escrow pending

completion of the transaction. The escrow was in a wallet maintained by Silk Road.

39. Once the transaction was complete, the user's Bitcoins were transferred to the Silk Road Bitcoin address of the vendor involved in the transaction. The vendor could then withdraw Bitcoins from the vendor's Silk Road Bitcoin address by sending them to a different Bitcoin address, outside Silk Road, such as the address of a Bitcoin exchanger who could exchange Bitcoins for a common currency.

40. The Silk Road charged a commission for every transaction conducted by its users. The commission rate varied, generally between 8 and 15 percent, depending on the size of the sale. Typically, the larger the sale, the lower the commission charged by Silk Road.

41. The Silk Road used a "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Blockchain. According to the Silk Road wiki, the Silk Road's tumbler "sent all payments through a complex, semi-random series of dummy transactions ... making it nearly impossible to link your payment with any coins leaving the site." In other words, if a buyer made a payment on Silk Road, the tumbler obscured any link between the buyer's Bitcoin address, the vendors Bitcoin address, and where the Bitcoins ended up. This made it fruitless to use the Blockchain to follow the money trail involved in the transaction, even if the buyer's and vendor's Bitcoin addresses were both known. The tumbler placed the Bitcoins utilized in a

given transaction into several different unknown Bitcoin wallets, which contained many more Bitcoins. Those Bitcoins were then sent to several other Bitcoin addresses in varying amounts. This took place until the original transaction's Bitcoins arrived in their final destination. Based on my training, experience, and this investigation, I know that the only function served by such "tumblers" was to assist with the laundering of criminal proceeds.

Bitmessage

42. Bitmessage is a decentralized, peer-to-peer, communications protocol that is used to send encrypted messages from one person to another or from one person to multiple persons.

43. Bitmesssage works by encrypting all incoming and outgoing messages using public key cryptography. Public key cryptography ensures that only the recipient of a message is capable of decrypting the message.

44. Bitmessage maintains anonymity between users by replicating all messages sent and received inside the network, therefore mixing all the encrypted messages sent by all the users of the network making it difficult to track which particular Bitmessage user sent a particular message and which user that message is destined for. Bitmessage addresses are made up of seemingly random character strings and resemble a Bitcoin wallet addresses. Bitmessage addresses are generated in this manner to ensure strong encryption and to avoid a user identity being revealed by his or her Bitmessage address.

45. Because all messages sent over the Bitmessage network are received by all users of the network, each instance of Bitmessage attempts to decrypt every message sent through Bitmessage, regardless its origin and destination. Since the intended recipient is the only user capable of decrypting the message, it is unnecessary for individual Bitmessages to be addressed to a recipient.

46. Because Bitmessage is peer-to-peer and decentralized in nature, it prevents any sensitive information being stored on a single server. All information is collectively stored throughout the network, and thus, there is no single failure point for the network. All unreceived Bitmessage messages are purged from the network after two days, preventing a buildup of stored messages.

47. According to http://bitmessage.org/, Bitmessage is specifically designed to hide non-content data, such as the sender and recipient of messages from intercept and passive eavesdropping.

Probable Cause

Background of Silk Road vendor CALIGIRL

48. Based upon my knowledge of the Silk Road website, I became familiar with a drug vendor who operated on the Silk Road under the username "CALIGIRL." CALIGIRL opened a Silk Road vendor account on April 10, 2013. Silk Road vendors were provided with a personal web space on which to advertise their products for sale and to display any messages they wished to

display. Feedback from previous buyers left for the vendor was also displayed on the vendor's page. A screenshot of CALIGIRL's offerings as of July 11, 2013 is attached to this affidavit at Exhibit 2.

49. CALIGIRL offered various controlled substances for sale, including Oxycodone,[3] Hydrocodone,[4] and Benzodiazepines. CALIGIRL stated that the Oxycodone products offered for sale were export products that did not contain safety measures designed to prevent intentional abuse and overdose. Based on my training and experience, Oxycodone that does not contain safety measures is preferred by drug traffickers, due to its higher demand and higher sales price. It is preferred by abusers as there are no chemical anti-abuse measures to defeat while ingesting the product.

Silk Road sales analysis for CALIGIRL

50. Between April 10, 2013 and September 9, 2013, the CALIGIRL Silk Road account completed 685 finalized sales. From these transactions, CALIGIRL collected Bitcoins valued at approximately $141,086.19. CALIGIRL also completed additional Silk Road sales valued at approximately $36,166.05 that were not finalized by the buyer or the funds remained in escrow. The Bitcoin to dollar price was calculated at time of each transaction and was recorded on the Silk Road server.

---

3 Oxycodone is a Schedule II controlled substance.

4 Hydrocodone is a Schedule II/III controlled substance.

51. As CALIGIRL completed 900 Oxycodone orders, 608 Hydrocodone orders, 165 Clonazepam[5] orders and 260 orders for other substances labeled "Prescription," "Pain Relief," "Drugs," "Adderall,"[6] "Benzos," "Tramadol," and "Lorazepam," each finalized sale likely contained multiple products in varying quantities.[7] The transactions were as follows:

- 24 identified transactions took place in April 2013 with an approximate Bitcoin value of $2,583.19;
- 6 identified transactions took place in May 2013 with an approximate Bitcoin value of $1,030.73.
- 53 identified transactions took place in June 2013 with an approximate Bitcoin value of $9,247.72.
- 225 identified transactions took place in July 2013 with an approximate Bitcoin value of $47,741.31;
- 256 identified transactions took place in August 2013 with an approximate Bitcoin value of $58,324.98; and
- Between September 1, 2013 and September 9, 2013, 219 identified transactions took place with an approximate Bitcoin value of $54,373.84.

52. The price of Bitcoin fluctuates in a manner similar to a stock or equity price. The average Bitcoin to U.S. dollar value between April 10, 2013 and September 9, 2013 was approximately $122.00.[8] The average Bitcoin to U.S. dollar value between September 10, 2013 and February 1, 2014 was

---

5 Clonazepam is a Schedule IV controlled substance.

6 Adderall (Mixed Amphetamine Salts) is a Schedule II controlled substance.

7 Lorazepam is a Schedule IV controlled substance.

8 http://www.bitcoinexchangerate.com/ average

approximately $817.00.[9] Utilizing the average price of Bitcoin for the above identified Silk Road transactions, between September 10, 2013 through February 1, 2014, the transactions were worth approximately $1,152,367.48.[10]

53. Based on my training and experience, drug traffickers acquiring large amounts of Bitcoin generally do not immediately attempt to exchange the Bitcoin into a national currency. Additionally, drug traffickers will generally exchange small amounts of Bitcoin into dollars, partaking in multiple, smaller transactions to avoid raising the suspicions of banks and triggering currency reporting requirements. Furthermore, exchanging large amounts of Bitcoins into a national currency in larger transactions may require photo identification be provided. As a result, those transactions are also avoided by drug traffickers.

Undercover Purchases and Seizures of Controlled Substances

54. Between July 11, 2013 and March 20, 2014, I completed eight (8) undercover purchases of controlled substances from CALIGIRL.[11] The undercover orders were placed both on the Silk Road website, utilizing an undercover user account I created and maintained, and through the Bitmessage program, utilizing an undercover identity I created on that network.

55. For the purchases made through the Silk Road website, I utilized the TOR browser to access the Silk Road website. Once on the Silk Road

---

9 http://www.bitcoinexchangerate.com/ average.

10 Because of the fluctuation of values, a Bitcoin value at time of transaction is not necessarily their value at time of their ultimate exchange to U.S. dollars.

11 I placed an additional two (2) undercover purchase orders which were subsequently cancelled by CALIGIRL due to supply issues.

website, I activated the links which lead me to CALIGIRL's vendor profile page. CALIGIRL's vendor profile page displayed various controlled substances for sale. The vendor page also displayed information that was posted by CALIGIRL that would assist potential customers in placing a successful order with CALIGIRL for controlled substances. Additionally, the vendor profile page contained feedback left by the vendors other customers. A screen capture of CALIGIRL's vendor profile page, captured on September 22, 2013, is attached to this affidavit as Exhibits 3-A, 3-B, 3-C, and 3-D.

56. For the purchases made through the Bitmessage program, I utilized a Bitmessage address provided to me by CALIGIRL. On October 9, 2013, I utilized the TOR browser to access the Silk Road forums. On the Silk Road forums, I located a post made by CALIGIRL's Silk Road account in a message thread titled "Vendors/Buyers - Post Future Details and Profiles Here – 3rd Backup Released." The purpose of this message thread was to provide buyers and vendors on the Silk Road website with a means to continue business, despite the shut down and seizure of the Silk Road website. In the message posted by CALIGIRL, an e-mail address of cg1@safe-mail.net and a Bitmessage address were provided.

57. On October 9, 2013, I sent a message to the Bitmessage address that was provided by CALIGIRL. CALIGIRL responded to my message by requesting my identity. I provided CALIGIRL with my undercover identity. CALIGIRL responded by providing me with a "trusted" Bitmessage address and

instructions to remove the original address. CALIGIRL further stated that future orders for controlled substances made through Bitmessage would be honored.

i. *July 11, 2013 undercover purchase of Oxycodone and Hydrocodone*

58. On July 11, 2013, I located two advertisements placed by CALIGIRL on the Silk Road website. The first advertisement was for "lots" of 10 OxyContin[12] 20mg tablets. Each lot of ten tablets was offered for sale in exchange for 2.3461 Bitcoins. At the time of transaction, 2.3461 Bitcoins was worth approximately $408.22. I added two lots of 10 OxyContin 20mg tablets (for a total of 20 20mg tablets) to my undercover "Shopping Cart" by activating the "Add to Cart" function.

59. The second advertisement was for 30 lots of Hydrocodone/Ibuprofen[13] 5/200mg. Each lot of 30 tablets was offered for sale in exchange for 1.6566 Bitcoins. At the time of transaction, 1.6566 Bitcoins was worth approximately $144.12. I added one lot of 30 Hydrocodone/Ibuprofen 5/200mg tablets to my undercover "Shopping Cart."

60. From an undercover Bitcoin wallet that I maintained, I transferred an appropriate amount of Bitcoins to the undercover Silk Road account Bitcoin wallet address. Once the Blockchain confirmed the Bitcoin transfer, I activated

---

[12] Oxycontin is a brand name for Oxycodone. Oxycodone is a Schedule II controlled substance.

[13] Hydrocodone is a Schedule III controlled substance when in combination with an additional medication.

the checkout function on the Silk Road website which prompted me for a shipping address and secret pin number.

61. I entered an undercover name and an undercover commercial post office box as the shipping address.[14] I then entered the secret pin associated with the undercover Silk Road account and completed the transaction. As a result, the Bitcoins appearing in my undercover Silk Road account wallet were removed and placed into the Silk Road escrow system. The Silk Road website assigned unique identification numbers to the order.

62. On July 15, 2013, I received a USPS priority mail package at the undercover commercial post office box location that I provided CALIGIRL as the shipping address for the Oxycodone and Hydrocodone tablets purchased on July 11, 2013. The box showed a handwritten return address of, "A. Wilson, 2071 N. Collins, Richardson, Texas 75080." The USPS tracking number showed the package originated in Fort Worth, Texas on July 11, 2013. The package had $5.80 postage affixed, in the form of one $5.60 "Arlington Green Bridge" stamp and two $0.10 stamps.[15]

63. Contained inside the USPS Priority package was an unmarked, sealed manila padded envelope. The manila envelope contained two clear

---

[14] The undercover commercial post office box utilized was located in Seminole County, Florida.

[15] Based on my training and experience, I know that drug traffickers prefer to use stamps to send shipments of controlled substances as it prevents them having to physically enter a post office or a commercial packing store. By entering a store, drug traffickers run the risk of being captured on closed-circuit video surveillance or recognized by staff.

plastic baggies, each containing pharmaceutical pills. The first baggie contained 20 Oxycodone 20mg tablets, each stamped with "EX" and "20." These markings are consistent with Oxycodone 20mg tablets manufactured for markets outside of the United States. The second baggie contained 31 Hydrocodone/Ibuprofen 5/200mg tablets. Each tablet was marked with a "X" style double-score. These markings are consistent with Vicoprofen which is manufactured for markets outside of the United States.

ii. *September 25, 2013 undercover purchase of Oxycodone*

64. On September 25, 2013, I located an advertisement placed on the Silk Road website by CALIGIRL that offered lots of 10 Oxycodone 20mg tablets in exchange for 1.5156 Bitcoins per lot, plus 0.054 Bitcoins for shipping. At the time of transaction, 1.5697 Bitcoins was valued at approximately $203.58. I added one lot of 10 Oxycodone 20mg tablets to my undercover "Shopping Cart" by activating the "Add to Cart" function.

65. From an undercover Bitcoin wallet that I maintained, I transferred an appropriate amount of Bitcoins to the undercover Silk Road account Bitcoin wallet address. Once the Blockchain confirmed the Bitcoin transfer, I activated the checkout function on the Silk Road website which prompted me for a shipping address and secret pin number.

66. I entered an undercover name and an undercover commercial post office box as the shipping address. I then entered the secret pin associated with the undercover Silk Road account and completed the transaction. As a result,

the Bitcoins appearing in my undercover Silk Road account wallet were removed and placed into the Silk Road escrow system. The Silk Road website assigned unique identification numbers to the order.

67. On September 30, 2013, I received a USPS Priority envelope at the shipping address I provided CALIGIRL for the shipment of Oxycodone purchased on September 25, 2013. The Priority envelope had a printed return address of "Kara Shea, Travel Professionals, 4903 W. Plano Pkwy, Plano, TX 75093." The affixed USPS tracking number showed the package originated at the Coppell, Texas[16] mail sort facility on September 26, 2013. The envelope had $5.60 in postage affixed, in the form of one "Arlington Green Bridge" $5.60 stamp.

68. Contained in the USPS Priority envelope was a sealed, padded manila envelope. Inside the manila envelope, I recovered two pharmaceutical blister packs, each containing 5 Oxycodone 20mg tablets. The blister packs, which were sealed, appeared to have been obtained directly from a pharmacy, were printed in Spanish, and indicated the tablets were manufactured by HumaX. HumaX is a pharmaceutical company operating in South America.

iii. *October 9, 2013 undercover purchase of Hydrocodone*

69. On October 9, 2013, I made contact with CALIGIRL utilizing the Bitmessage program and the "trusted" Bitmessage address CALIGIRL provided me. CALIGIRL offered to sell me 50 Hydrocodone/Ibuprofen 50/200mg tablets in

[16] The Coppell, Texas U.S. Mail sort facility is located in zip code 75099. This zip code is reserved solely for the sort facility. Tracked mail originating from this location would placed into a collection box and did not pass over a USPS counter.

exchange for 1.65 Bitcoins. At the time of transaction, 1.65 Bitcoins were valued at approximately $206.98.

70. I agreed to purchase the 50 Hydrocodone/Ibuprofen tablets in exchange for 1.65 Bitcoins and sent the agreed upon number of Bitcoins to the Bitcoin wallet address CALIGIRL provided. I provided CALIGIRL an undercover commercial post office box as the shipping address.

71. On October 17, 2013, I received a USPS Priority Mail envelope at the undercover address I provided CALIGIRL for the Hydrocodone tablets purchased on October 9, 2013. The USPS Priority envelope had a printed return address of, "Tyler Randolph, Northwest Insurance, 616 N. Central Expressway, Dallas, TX 75206." The USPS tracking number affixed indicated the package had originated at the Coppell, Texas mail sort facility on October 9, 2013. The envelope had $5.60 in postage affixed to it in the form of one "Arlington Green Bridge" $5.60 stamp.

72. Contained inside the USPS Priority envelope, I located a sealed, padded manila envelope. The manila envelope contained a clear plastic baggie, which contained 50 Hydrocodone/Ibuprofen 5/200mg tablets. The tablets were of the exact same type previously obtained from CALIGIRL.

iv. *October 22, 2013 undercover purchase of Hydrocodone*

73. On October 22, 2013, I again made contact with CALIGIRL through the Bitmessage program and the "trusted" Bitmessage address CALIGIRL provided me. CALIGIRL offered to sell me 50 Hydrocodone/Ibuprofen 50/200mg

tablets in exchange for 1.06 Bitcoins, valued at approximately $200 at time of transaction.

74. I agreed to purchase 50 Hydrocodone/Ibuprofen 5/200mg tablets in exchange for 1.06 Bitcoins that I sent to the CALIGIRL's Bitcoin wallet address. I provided CALIGIRL with an undercover commercial post office box for use as the shipping address.

75. On October 25, 2013, I received a USPS Priority mail envelope at the shipping location provided to CALIGIRL for the Hydrocodone tablets purchased on October 22, 2013. The USPS Priority envelope had a printed return address of, "McKinsey & Co, 2200 Ross Ave, Dallas, Texas 75201." The USPS tracking number affixed showed the package originated at the Coppell, Texas mail sort facility on October 22, 2013. The envelope had $5.60 in postage affixed, in the form of one "Arlington Green Bridge" $5.60 stamp.

76. Contained inside the USPS Priority envelope was a sealed, padded manila envelope. Inside the manila envelope, I recovered a clear plastic baggie, which contained 50 Hydrocodone/Ibuprofen 5/200mg tablets. The tablets were the exact same kind as those I previously received from CALIGIRL.

v. *January 3, 2014 undercover purchase of Oxycodone and seizure of packages at postal facility*

77. On January 3, 2014, I made contact with CALIGIRL utilizing the Bitmessage program and the "trusted" Bitmessage address that CALIGIRL previously provided. CALIGIRL offered to sell me 100 generic Oxycodone 20mg

tablets in exchange for Bitcoins worth $1,400. CALIGIRL stated that, for an additional $200, name brand tablets would be supplied.

78. I agreed to purchase 100 generic branded Oxycodone 20mg tablets, in exchange for 1.755 Bitcoins which were valued at approximately $1,400 at the time of transaction. CALIGIRL provided me with a Bitcoin wallet address to which I sent the agreed upon number of Bitcoins. I requested that the order not be shipped until January 23, 2014.

79. On January 13, 2014, I went to the Coppell, Texas USPS processing plant. Because all of the undercover purchases of controlled substances, except one,[17] originated at the Coppell, Texas mail processing plant, Postal Inspectors and I attempted to profile additional packages that could match packages originating with CALIGIRL.

80. A total of four (4) packages matching the profile were removed from the postal stream. The four packages removed all originated from a blue U.S. Mail collection box located at 8135 Forest Lane, Dallas, Texas. That location was approximately 0.4 miles from Jones' residence at the time of the shipment, 12009 Coit Road, Apartment 5313M, Dallas, Texas.

81. All four of the packages had a printed return address of, "Andrea Peterman, Sheraton Dallas, 400 N. Olive Street, Dallas, TX 75201." The packages all had tracking numbers affixed; however, they were removed from the postal stream prior to entrance in to the USPS tracking system.

---

[17] The exception was the undercover purchase made on July 11, 2013.

82. One of the packages removed from the Coppell, Texas mail processing plant was the package addressed to my undercover identity. Contained in the package was a padded, sealed manila envelope. Inside the manila envelope was a clear plastic baggie containing 100 Oxycodone 20mg tablets.

83. The additional three (3) packages were addressed to Customer-1, Customer-2, and Customer-3. Federal search warrants, issued by the United States Court, Northern District of Texas, were executed on the additional packages. All three packages were found to contain controlled substances. Specifically, the packages contained:

- Customer 1: 22 brand name Oxycodone 20mg tablets, 10 Hydrocodone/Ibuprofen 5/200mg tablets and 10 Clonazepam[18] tablets.
- Customer 2: 3 brand name Oxycodone 20mg tablets, 25 brand name Oxycodone 10mg tablets, 3 generic Oxycodone 20mg tablets, 4 generic Oxycodone 40mg tablets, and 3 brand name Oxycodone 40mg tablets.
- Customer 3: 10 Oxycodone 20mg tablets.

vi. *January 23, 2014 "replacement" shipment of Oxycodone*

84. In response to the package that I purchased on January 3, 2014, which was marked as undelivered due to its removal from the postal stream, CALIGIRL agreed to send me a replacement shipment of 100 Oxycodone 20mg tablets. I provided CALIGIRL with an undercover commercial post office box as a shipping address. I did not provide CALIGIRL with any Bitcoins for this replacement order.

[18] Clonazepam is a Schedule IV controlled substance.

85. Also on January 13, 2014, I accompanied a U.S. Postal Inspector to E-Z Mail Services.[19] While at E-Z Mail services, the owner/manager[20] stated there was a suspicious package in mailbox 620. Inside the mailbox, I observed a small USPS Priority flat rate package that was addressed to Tyler Zeddai. All seams of the box were taped excessively. A federal search warrant, issued by the United States District Court, Northern District of Texas, was executed on the package. Inside the box, I located a "calm aid" box and a printed shipping invoice for a natural calming product. Concealed inside the "calm aid," I recovered 685 Hydrocodone 5mg tablets. The tablets were marked "Hycodan."[21]

86. On January 23, 2014, I received a USPS Priority mail envelope at the shipping address I provided CALIGIRL for the re-shipment order. The USPS Priority envelope had a printed return address of, "Beading Dreams, 5929 W. Lovers Lane, Dallas, TX 75029." The USPS tracking number affixed indicated the shipment originated in Coppell, Texas on January 21, 2014. The envelope had $5.66 of postage affixed to it in the form of one $5.00 stamp and two $0.33 stamps.

87. Contained in the USPS Priority envelope was a sealed, padded manila envelope. Contained inside the manila envelope was a clear plastic baggie containing 100 Oxycodone 20mg tablets.

---

19 As detailed later in this affidavit, mailbox 620 at E-Z Mail Services is leased by Jones.

20 According to the owner/manager of E-Z Mail Services, he/she is familiar with his/her customers.

21 Hydrocodone in this form is Schedule II controlled substance.

vi. *February 5, 2014 undercover purchase of Hycodan and Oxycodone*

88. On February 5, 2014, I again made contact with CALIGIRL through the Bitmessage program, and the "trusted" Bitmessage address CALIGIRL supplied to me. CALIGIRL offered to sell me Hydrocodone 5mg tablets which were not combined with any additional medications. CALIGIRL stated this was a "balloon test" order and that the Hydrocodone was offered for sale at a price of Bitcoins valued at $275 per 50 tablets. CALIGIRL also offered Oxycodone products for sale Oxycodone.

89. I agreed to purchase 50 Hydrocodone 5mg tablets and 100 Oxycodone 20mg tablets in exchange 2.102 Bitcoins, valued at approximately $1,675 at time of transaction. CALIGIRL provided me a Bitcoin wallet address to which I transferred the appropriate amount of Bitcoins.

90. On February 6, 2014, I received a Bitmessage message from CALIGIRL. In the message, CALIGIRL informed me that the Hydrocodone 5mg tablets I purchased were branded "Hycodan." CALIGIRL provided me a link to a pill identification website which showed a picture of the tablets. The branding and picture supplied by CALIGIRL matched the Hycodan Hydrocodone tablets seized on January 13, 2014 from Jones' E-Z Mail Services mailbox and addressed to Tyler Zeddai.

91. On February 10, 2014, I received a USPS Express mail envelope at the shipping address I provided CALIGIRL on February 5, 2014. The express mail envelope had a handwritten return address of, "Stewart Title, 12700 Preston

Rd, Dallas, TX 75230." The USPS tracking number affixed indicated that the package originated at the Coppell, Texas sort facility on February 8, 2014. The envelope had $20.00 of postage affixed in the form of four $5.00 stamps.

92. Contained inside the Express Mail envelope was a sealed, padded manila envelope. Inside the manila envelope were two clear plastic baggies. One plastic baggie contained 100 Oxycodone 20mg tablets. The second plastic bag contained 50 Hydrocodone 5mg tablets. The Hydrocodone tablets were branded "Hycodan" and matched tablets seized from the Arlington, Texas mailbox on January 13, 2014 and the pill identification information provided by CALIGIRL on February 6, 2014.

vii. *March 18, 2014 undercover purchase of Oxycodone and Hycodan Hydrocodone; Automatic Postal Center photograph of Jones*

93. On March 17, 2014, I again made contact with CALIGIRL through the Bitmessage program and the "trusted" Bitmessage address CALIGIRL supplied to me. I informed CALIGIRL that I wanted to purchase 100 Oxycodone 20mg tablets and 100 "Hycodan" Hydrocodone 5mg tablets, but that I only had in my possession 1.4 Bitcoins which would not cover the cost.

94. In response, CALIGIRL stated that I should contact Matthew Jones and provided me a telephone number of 972-666-1223 for Jones. Further, CALIGIRL stated that Jones was also known as "DYNAMITE2k" on http://localbitcoins.com/ and would be able to accept cash from me, as well as, provide Bitcoins for the purchase of controlled substances.

95. I contacted Jones on the telephone number provided. Jones stated that he liked to speak to new Bitcoin clients to ensure that both parties understood Jones' process and that there were "no surprises." I told Jones that I wanted to provide him $1,000 to convert into Bitcoins and then transfer to CALIGIRL. Jones referred to CALIGIRL as "Jen."

96. Jones stated that he would provide me with a Wells Fargo Bank account number and account holder name via text message after the conclusion of our phone call. Jones instructed me to go to a Wells Fargo Branch location and deposit the currency directly into the account he provided. Jones told me not to put any information additional to the account holder name and account number, and to not answer any questions that may be asked by the bank teller. After the deposit was completed, Jones instructed me to send him a picture of the deposit slip.

97. Shortly after the conclusion of the telephone call, Jones sent me a text message in which he provided me a Wells Fargo Bank savings account number that was held in the name of "Jonathan Lopez."

98. On March 18, 2014, I went to the Wells Fargo Bank branch located at 1530 International Parkway, Lake Mary, Florida. I completed a bank deposit slip with the information provided by Jones. I gave the deposit slip and $1,000 to the bank teller. The bank teller provided me with a deposit receipt. I took a picture of the deposit slip and sent it via text message to Jones. In addition to

the photograph that I provided to Jones, Jones stated via text message that he also contacted the bank to confirm the deposit.

99. I asked Jones to confirm the actual amount of Bitcoins that would be credited towards future purchases. Jones stated that I should think in terms of cash, and that, after a 5% commission, $952.38 would be credited towards future purchases. Based on my training and experience, Jones' statements indicated that no conversion to Bitcoin was taking place; Jones was both the recipient of the currency and the sender of the controlled substances.

100. On March 28, 2014, I attempted to contact CALIGIRL through Bitmessage to make a change to the order of 100 Oxycodone 20mg tablets and 100 Hydrocodone 5mg tablets. Through Bitmessage, CALIGIRL stated that the order had already shipped at a cost of $1,900 with $952 credited towards the purchase.

101. I agreed to the purchase but stated that I only possessed 1.41 Bitcoins which would be approximately $55.00 short of the $1,900 purchase price. CALIGIRL stated that since the order had already shipped, the difference in balance could be rectified at a later date. CALIGIRL provided me with a Bitcoin wallet address into which I transferred 1.41 Bitcoins to complete the transaction.

102. On March 20, 2014, I received a USPS Priority Mail envelope at the undercover commercial mailbox that I provided as a shipping address on March 18, 2014. The USPS Priority Mail envelope had a tracking number affixed to

it. The tracking number indicated the package received its first scan at the Coppell, Texas sort facility at 10:00 p.m. on March 18, 2014. Also affixed to the envelope was an Automated Postal Center[22] ("APC") computer generated postage stamp valued at $5.60. The APC postage indicated a purchase date of March 17, 2014 and a purchase zip code of 75260. The APC machine was located at the Dallas Main Post Office, 401 Dallas Fort Worth Turnpike, Dallas, Texas 75260. The USPS Priority envelope had a printed return address of "Tonya Berent, LPC, 9323 Dove Meadow Dr., Dallas, TX 75243" affixed to it.

103. Contained in the USPS Priority Mail envelope was a sealed manila envelope. Contained inside the manila envelope were two clear plastic baggies. One baggie contained 100 Oxycodone 20mg tablets. The other clear plastic baggie contained 100 "Hycodan" Hydrocodone 5mg tablets. The Oxycodone 20mg tablets and the "Hycodan" Hydrocodone 5mg tablets were identical to those previously purchased through both the Silk Road webpage and through the CALIGIRL Bitmessage account.

104. The United States Postal Inspector service subsequently provided me with the images captured by the APC machine during the purchase of the postage affixed to the package I received on March 20, 2014. I compared the APC images to known images of Jones, including publically available images on

[22] APC machines are similar to Bank Automatic Teller Machines, and allow users to undertake basic postal transactions without having to go to the post office counter. APC machines generally capture images of their users at time of transaction.

Facebook[23] and found them to match. Additionally, I showed the images to DEA TFAs who have previously seen Jones in person. These agents also confirmed that the photographs depicted Jones.[24]

105. As part of this investigation, I reviewed telephone toll information for 972-666-1223 obtained from Dingtone, Inc. (Dingtone[25]). Telephone number 972-666-1223 was the number that CALIGIRL told me to call when I needed to speak to Jones.

106. The Dingtone records contained information regarding the download, activation, and purchase of calling plans for the account associated with telephone number 972-666-1223. The records also contained voice and SMS connection records. The records did not contain any conversation or content data.

107. According to the records, Matthew Jones purchased the calling plan and was assigned telephone number 972-666-1223 at 7:20 p.m. GMT, which was 3:20 p.m. EDT. Jones purchased the calling plan and telephone

---

[23] http://www.facebook.com/mateo.Jones.5 and http://www.facebook.com/matthewdpi are the Facebook profiles belonging to Jones. Both Facebook accounts contain publically viewable photographs of Jones.

[24] The photograph is attached to this affidavit as Exhibit 4.

[25] Dingtone is an application for smartphone devices, for which a user can be assigned an actual telephone number for making and receiving telephone calls and text/multimedia messages over the internet. Since the transfer takes place over the Internet, it is possible to have multiple telephone numbers on one cellular telephone and not utilize the cellular telephone number assigned by the cellular provider. In the case of Apple iPhone devices, the Dingtone application is downloaded through the Apple App Store. Individuals who download the application have the option of purchasing a calling plan and would be purchased through the Apple App Store.

number approximately one minute before providing it to me through Bitmessage under the name CALIGIRL.

108. The records further detailed that the application was installed on an Apple iPhone that was titled "Matthew Jones iPhone." The records detailed that the account username was "Matthew Jones." At time of signing up for the service, Jones provided his cellular telephone number, 214-810-0295. The cellular number Jones provided was the same number utilized to receive a confirmation of account SMS text message from Dingtone.

109. According to the records, the first and only outgoing call that was ever placed utilizing the account was to my undercover telephone number. This call was placed on March 17, 2014 at 4:31 p.m. and went unanswered.

110. Jones received three incoming calls that were answered. One call was from me and is detailed in this affidavit. The additional answered incoming telephone calls appear to have been from telemarketers.[26]

111. The Dingtone records also included data regarding the SMS messages sent and received by 972-666-1223. The only SMS messages sent or received from the account were to and from my undercover telephone number.

112. The Dingtone records also included IP addresses utilized to log in to the application between March 18, 2014 and March 28, 2014. During that

[26] Research of these additional telephone numbers revealed that they were from cold-call telemarketers and/or telephone scams. Both telephone numbers were disconnected prior to April 8, 2014.

reporting period, Jones logged in to the application from IP addresses associated with Cingular Wireless, Roadruner Internet Texas, Data Paradigm,[27] and IP addresses in Colombia.

Package Profile

113. By examining the packages seized at the Coppell, Texas sort facility on January 13, 2014, it was determined that a number of packages containing controlled substances mailed by Jones/CALIGIRL were placed into the USPS collection box located at 8135 Forest Lane, Dallas, Texas. Specifically, when the USPS collects items from a USPS collection box, the items are placed into a bin that has the collection location affixed to it. This collection box is located approximately 0.4 miles from Jones' former home address, 12009 Coit Road, Apartment 5313M, Dallas, Texas.[33]

114. Additional packages identified through the package profile were identified as originating in the Dallas metropolitan area and in Port Isabel, Texas.

115. The package profile associated with Jones/CALIGIRL was further developed by comparing the packages received during controlled purchases and examining any commonalities between the packages. Known packages originating with Jones had affixed USPS tracking numbers which were printed in and circulated in groups. These known packages had affixed tracking numbers in the same group and had additional features that remained consistent

---

27 As stated in this affidavit, Data Paradigm is Jones' employer.

33 On or about February 17, 2014, Jones moved to his current home address, 13625 Far Hills Lane, Dallas, Texas.

throughout the investigation. The features that remained consistent included the manner in which the sender and recipient addresses were printed and affixed, the placement and method of postage, and the type of envelope utilized.

116. On each of the parcels, postage was paid for by the utilization of $5.00+ face-value stamps and the tracking numbers were affixed prior to mailing. Based on my training and experience, these methods permit Jones from having to pass packages containing controlled substances over a Post Office counter which would risk Jones' identification by postal staff or capturing of his image on USPS video surveillance systems. The only exception was the postage affixed to the March 18, 2014 undercover controlled purchase, which had APC printed postage.

117. Additionally, through the package profile developed and detailed in this affidavit, numerous other packages originating with Jones were identified. Each of these packages had a return address affixed. The return addresses affixed to the packages were real addresses in the Dallas, Texas area, but addresses to which Jones had little or no association. The identified return addresses were:

- 2071 N. Collins, Richardson, TX 75080
- 7675 Main St., Dallas, TX 75207
- 2602 McKinney Ave., Dallas, TX 75204
- 1246 Brown Blvd., Arlington, TX 76011
- 5301 W. Lovers Lane, Dallas, TX 75209

- 4903 W. Plano Parkway, Plano, TX 75093
- 12720 Merit Dr., Dallas, TX 75251
- 11822 Neering Dr., Dallas, TX 75251
- 11827 Neering Dr., Dallas, TX 75251
- 9040 Garland Rd., Dallas, TX 75218
- 616 N. Central Expressway, Dallas, TX 75206
- 13305 Meandering Way, Dallas, TX 75240
- 13220 Maham Rd., Dallas, TX, 75240
- 2200 Ross Ave., Dallas, TX 75201
- 3406 Oak Lawn Ave., Dallas, TX 75219
- 400 N Olive St, Dallas, TX 75201
- 5929 W Lovers Lane, Dallas, TX 75029
- 12700 Preston Rd., Dallas, TX 75230
- 9323 Dove Meadow Dr., Dallas, TX 75243

118. Each of the above return addresses was utilized for a block of packages mailed by Jones. Packages mailed within approximately seven (7) days of each other contained the same return address. After the grouping of packages was sent, a new return address was utilized.

119. Utilizing the package identification profile, a total of 135 packages were identified as having originating with Jones. Each of the packages identified had one of the above return addresses affixed.

Mail Drop/Receipt Locations Utilized by Jones

U.S. Mail Facility - 8135 Forest Lane, Dallas, Texas

120. The U.S. Mail facility located at 8135 Forest Lane, Dallas, Texas is the known origination point for at least five known controlled substance shipments sent by Jones. This point of origin was determined by the profiling of incoming mail at the Coppell, Texas mail processing plant on January 13, 2014. As mail is collected from collection points by the U.S. Mail, it is placed in to labeled bins that depict the point of mailing for the mail contained in the bin. All of the packages identified and seized on January 13, 2014 originated at 8135 Forest Lane, Dallas, Texas. Jones' current residence is located approximately 2.6 miles from the U.S. Post Office drop box located at 8135 Forest Lane, Dallas, Texas.

E-Z Mail Services - 1861 Brown Boulevard, Box 620, Arlington, Texas 76006

121. During my investigation, I identified a commercial mailbox leased by Jones located at 1861 Brown Boulevard, Box 620, Arlington, Texas 76006. This mailbox is located inside an E-Z Mail Services, Inc. store. E-Z Mail Services is a commercial packing store that rents personal mailboxes. The lease, which I obtained from the United States Postal Inspection Service, originated on May 4, 2007 and the mailbox was opened in the names of Jones and "Tyler Zeddai." Two forms of identification were required to open the commercial mailbox. Jones

provided his Texas driver's license and a VISA debit card bearing his name. No identification was provided by "Tyler Zeddai."[35]

122. The owner/manager of E-Z Mail Services stated that he had never seen Tyler Zeddai. According to the manager/owner, only Jones and his spouse, "P.C.E.," had ever removed items from the mailbox. According to the owner/manager, Tyler Zeddai regularly received packages at the mailbox, however, those packages were removed from the mailbox by Jones.

123. The owner/manager of EZ Mail Services further stated that, when Jones visited E-Z Mail to pick up mail and packages, he drove a 2000 black Honda CR-V. The Postal Inspector showed the owner/manager a picture of Jones' vehicle and the owner/manager recognized it as the same vehicle Jones drove to E-Z Mail Services.

124. The E-Z Mailbox location is approximately 26 miles from Jones' current home address, 13625 Far Hills Lane, Dallas, Texas, and approximately 19 miles from Jones' workplace. The mailbox is also located approximately 26 miles from Jones' previous home address, 12009 Coit Road, Apartment 5313M, Dallas, Texas.

---

[35] There is no record of a Tyler Zeddai in any state or federal identification database that I checked. A public records search for Tyler Zeddai returned the address of 1861 Brown Boulevard, Box 620, Arlington, Texas. Based on my investigation, I believe Tyler Zeddai does not exist and is an alias that is utilized by Jones.

Jones' Purchases of Packaging Materials on Amazon.com

125. During the course of this investigation, I reviewed records obtained from Amazon.com ("Amazon") relating to Jones' purchases from its website. The records reviewed included purchase, shipping, billing, and IP address information.

126. The records showed that, on July 2, 2013, Jones utilized his Amazon account to purchase 1000 3" x 5" clear plastic zip lock baggies and 500 4" x 8" bubble mailer manila envelopes.

127. I then reviewed the advertisements for these products on Amazon's website. When I compared the items to those that packaged the controlled substances that I purchased from CALIGIRL on Silk Road and Bitmessage, they matched. Additionally, the packages containing controlled substances obtained during this investigation, including those obtained through controlled purchases and those seized from the postal stream pursuant to federal search warrants, were all packaged in similar bubble envelopes and plastic baggies.

128. Jones utilized his Wells Fargo VISA debit card, xxxxxx6133, to complete the Amazon purchases. The billing address Jones provided was 1861 Brown Boulevard, Box 620, Arlington, Texas.

129. Jones completed the Amazon transaction from IP address 184.146.37.164. I geo-located this IP address to Colombia. As detailed in this affidavit, Jones is known to frequently travel to Colombia.

130. Jones has also accessed Bitcoin trading Internet chat rooms[36] from this IP address. Specifically, on March 24, 2013, Jones accessed the chat room "#bitcoin-otc" under the pseudonym "Dynamite`" from IP address 184.146.37.164.[37] Jones' was authenticated on the chat room by the Bitcoin-otc authentication software, providing proof that "Dynamite`" was indeed Jones and not someone attempting to utilize his pseudonym.

Public Domains Associated with Matthew Jones

131. I located a public profile for Jones at http://linkedin.com/in/matthewvJones.[38] On Jones' LinkedIn profile, he lists his employment as "Director of Technology/Consulting Services" at Data Paradigm.

132. I performed a "WHOIS" query on www.i-transact.com. This domain name forwards traffic to www.itransact.com, the official website of the iTransact Group, LLC. The domain name technical contact for www.i-transact.com was listed as "Netfire Operations Center" located at 2907 Forestwood Drive, Dallas, Texas 76006. This address is the address that appears on Jones' Texas driver's license. The telephone number listed for Netfire Operations Center was 214-853-5236 and matches a telephone number known to be utilized by Jones.

---

[36] Internet Relay Chat ("IRC") is an internet protocol that facilitates the transfer of text based messages between one or more parties. The protocol follows the client/server mode of networking facilitating the central distribution of text to single persons or groups of people.

[37] http://bitcoinstats.com/irc/bitcoin-otc/logs/2013/03/24.

[38] LinkedIn is a social networking website for people in professional occupations.

133. I utilized Jones' telephone number, 214-853-5236, to locate additional domain names registered by Jones. I located 12 additional domain names containing 214-853-5236 in the WHOIS records. Included in the list of domain names were www.arlingtonhardware.com, www.redi-check.com, and www.redicharge.com. All of these domains listed an address of 2602 McKinney Avenue, Dallas, Texas as the contact address. As detailed in this affidavit, the address 2602 McKinney Avenue, Dallas, Texas was utilized as the return address on a package identified by the United States Postal Inspector as originating with CALIGIRL. This package was placed in the mail stream on or about August 23, 2013.

North Texas Tollway Authority Records

134. During the course of this investigation, I reviewed Jones' records obtained from the North Texas Tollway Authority (NTTA). Jones uses a NTTA account and transponder. Jones' vehicle is the only vehicle listed on the account and Jones is the only person listed on the account.

135. The NTTA records that I reviewed covered the time period of August 24, 2013 through February 21, 2014. The toll charges incurred on the NTTA account detail that Jones' vehicle utilized NTTA roads to travel between Jones' former residence, 12009 Coit Road, Apartment 5313M, Dallas, Texas and Jones' commercial mailbox located at E-Z Mail Services.

136. Additionally, the NTTA records detailed that Jones' vehicle was regularly parked at the Dallas/Ft. Worth Airport during the dates Jones was known to be travelling to Medellin, Colombia.

Jones' International Travel to Colombia

137. During the course of the investigation, documents I obtained from Spirit Airlines and American Airlines detailed that Jones made frequent trips to Colombia and maintained various ties to that country.[39]

138. Between April 1, 2013 and March 6, 2014, Jones made the following trips to Colombia:

- April 7, 2013 - travel to Medellin, Colombia on Spirit Airlines
- April 26, 2013 - travel to Medellin, Colombia on Spirit Airlines
- June 20, 2013 - travel to Medellin, Colombia on Spirit Airlines
- July 12, 2013 - travel to Medellin, Colombia on Spirit Airlines
- August 29, 2013 - travel to Medellin, Colombia on Spirit Airlines
- December 22, 2013 - travel to Medellin, Colombia on COPA Airlines
- February 26, 2014 - travel to Medellin, Colombia on Spirit Airlines

139. The dates contained on Jones' travel itineraries were consistent with dates provided to me by CALIGIRL during undercover conversations taking place utilizing the Bitmessage program. The dates indicated during undercover conversations included dates when controlled substance shipments would not be mailed, due to CALIGIRL being on "vacation."

[39] Jones' spouse is a Colombian national.

Origin of Oxycodone Products Offered for Sale by CALIGIRL

140. Colombia is a source country for the Oxycodone products the Jones offers for sale. The packaging and markings of pills obtained during controlled undercover purchases confirm that they were manufactured in Columbia. Additionally, the manufacturer of the generic Oxycodone 20mg tablets purchased from Jones is HumaX, a Colombian pharmaceutical manufacturer. HumaX pills are not marked appropriately for import, sale, or distribution in the United States.Oxycodone and Hydrocodone products sourced from South America and imported in to the United States offer financial advantages to obtaining the product domestically. Oxycodone and Hydrocodone are easier to obtain and they cost significantly less than similar products obtained in the United States. Additionally, Oxycodone and Hydrocodone tablets manufactured outside the United States are not required to meet marking and anti-abuse standards required by the United States. Generic brands of Oxycodone, such as HumaX, are marked with a simple double score pattern making the tablet very difficult for law enforcement to identify the pill. Many non-controlled substances and dietary supplements in the United States share these double score marking, whereas domestic Oxycodone and Hydrocodone tablets have more distinct markings. Tablets are only able to be identified through careful inspection or laboratory analysis. As a result, tablets marked in this manner are preferred by drug traffickers due to decreased law enforcement scrutiny.

Financial Analysis

Jones' Use of Xoom for International Wire Transfers

141. During this investigation, I reviewed records obtained from Xoom Corporation regarding Jones' Xoom account. Xoom is an online wire transfer service that provides consumer currency remittance.

142. The records received covered the time period of January 1, 2012 through August 2, 2013. Jones' account listed the following information:

Name: Matthew Jones
Address: 1861 Brown Blvd., #620, Arlington, TX
Email: mJonesdpi@gmail.com
Phone: 214-810-0295

143. During this period, Jones sent Xoom wire transfers totaling $58,022.57 in a total of 131 transactions. Of these transactions, 128 transactions, totaling $57,472.57, were sent to Colombia. The remaining three transactions, totaling $550, were sent to Costa Rica. 31 of these transactions, totaling $20,979, were sent to "Mateo Jones," which is an alias utilized by Matthew Jones on Facebook. The average value of these transfers was $676.74. All of the wire transfers sent to "Mateo Jones" were received in BanColumbia account number xxxxxxx5028.

144. 57 of the Xoom transactions, totaling $27,091.07, were sent to "P.C.E.," Jones' spouse. The average value of these transfers was $475.28. All the wire transfers sent to "P.C.E." were received in BanColumbia account number xxxxxxx8311.

145. 19 of the Xoom transactions, totaling $5,174, were sent to "A.G.R." The average value of these transfers was $272.32. All of the wire transfers sent to "A.G.R." were received in BanColumbia account number xxxxxxx3764.

146. The transactions sent to "A.G.R." appeared to have been structured in a manner to intentionally avoid triggering money laundering and reporting requirements. There were multiple transactions made on the same day to the same person and there were several transactions over a short time frame to the same person. These transactions also appeared to have been structured in order to remove currency from the United States without triggering currency export reporting requirements.

147. The remaining transactions, totaling $4,251.50, had a consistent relationship between the sender and recipient of the funds. Additionally, the funds were sent in consistent amounts with the average transfer amount being $177.15.

148. 70 of the Xoom wire transfers, totaling $31,374.83, were funded utilizing Jones' Wells Fargo debit card xxxxxx6133. This card debited money from Jones' Wells Fargo account xxxxxx5888. Jones received statements for this Wells Fargo account at his E-Z Mail Services mailbox.

149. 40 of the Xoom wire transfers, totaling $15,537.74, were funded utilizing Jones' Diners Club card, xxxxxx5536. This card was issued to Jones by

BHO Harris Bank. Jones received statements for his Diners Club credit card at his E-Z Mail Services mailbox.

150. The remaining wire transfers were paid utilizing other debit and credit cards issued to Jones.

151. Jones discontinued utilizing Xoom's services after August 2, 2013.

152. As Xoom operates as an online service, the records they provided also included IP addresses that Jones' account was accessed from. I performed IP address lookups on the provided IP addresses. During the period Jones used Xoom, his account was accessed from IP addresses located in Dallas, Texas, Wilmington, North Carolina, and from IP addresses located in Colombia. The Xoom account was also accessed from IP address 38.107.218.2. I identified this IP address as assigned to the Sheraton Dallas Hotel. The Sheraton Dallas is located at 400 N. Olive Street, Dallas, Texas and is connected by elevated walkway to Jones' place of employment. The Sheraton Dallas was utilized as a return address on packages containing controlled substances, including several of the packages seized on January 13, 2014 at the Coppell, Texas U.S. Postal Service sort facility.

Wells Fargo Bank Accounts

153. As part of my investigation, I reviewed records obtained from Wells Fargo Bank NA, regarding accounts held by Jones.

A. Checking account xxxxxx5888 and savings account xxxxxx4421

154. I reviewed records for Wells Fargo account xxxxxx5888, a checking account opened by Jones on February 8, 2010. When opening the account, Jones provided his Texas driver's license, Social Security number, and a Citi Group MasterCard as forms of identification.

155. I also reviewed Wells Fargo savings account xxxxxx4421. Account xxxxxx4421 was opened at the same time as account xxxxxx5888.

156. The particular Wells Fargo Bank location where these accounts were opened, 1889 Brown Boulevard, Arlington, Texas, is less than 200 yards from Jones' E-Z Mail Services mailbox.

a. *2013 deposits analysis of xxxxxx5888*

157. Between January 1, 2013 and November 27, 2013, a total of $141,461.95 was deposited into account xxxxxx5888. Total monthly deposits averaged $12,860.17. The statement period of September 2013 contained the lowest total deposits, totaling $7,124.43. The statement period of October 2013 contained the highest total deposits, totaling $20,194.07.

158. Of these deposits, $70,140.38 appeared to be payroll deposits from Jones' employer, Data Paradigm. The deposits from Data Paradigm were for inconsistent amounts of money. The lowest deposit from Data Paradigm was $1,158.91 and the highest deposit from Data Paradigm was $5,270.31. An additional $5,175 was deposited in scheduled, consistent deposits from third-parties. The average value of those deposits was $345.

159. Other deposits into the account included $20,659.28 in cash deposits made at a Wells Fargo bank branch counter. An additional $10,853.56 was deposited at ATM machines. The Wells Fargo counter and ATM deposits were in inconsistent amounts, occurred on a variety of dates, and were made at a variety of geographical areas. Based on my training and experience, this activity is consistent with Bitcoin sales where a Bitcoin customer makes a pre-arranged counter-deposit into a Bitcoin dealer's bank account. The deposit slips contain only the minimum amount of information required to make a cash deposit. Based on my training, experience, and this investigation, this is a common behavior utilized by Bitcoin exchangers and drug traffickers when utilizing counter-deposits to transmit currency.

160. Bitcoin exchange deposits into the account totaled $7,493.71. Dwolla, an online Bitcoin exchange, deposits accounted for $6,409.71. Coinbase, another online Bitcoin exchange, deposits totaled $1,084.04. Notably, there were no Bitcoin related debits from any of the accounts I reviewed during any time period. Based on my training and experience, the lack of Bitcoin exchange debits is consistent with drug traffickers accepting Bitcoin as a method of payment. Drug traffickers accepting Bitcoin as payment accrue large numbers of Bitcoins through drug sales and, therefore, do not have to purchase any Bitcoin from Bitcoin exchangers.

b. 2013 debits analysis of xxxxxx5888

161. Between January 1, 2013 and November 27, 2013, a total of $137,083.70 was debited from account xxxxxx5888. The monthly debits averaged $12,462.15. The statement period of September 2013 contained the lowest total debits, totaling $4,375.25. The statement period of May 2013 contained the highest total debits, totaling $17,193.13. Of the $137,083.70 total debits, $11,765.16 were for rent and housing payments.

162. During this period, a total of $12,001.92 was debited from ATM machines in Colombia. Each individual transaction was mirrored the same day by at least one identical transaction.

163. During this time period, an additional $12,055.19 was debited by Xoom. The Xoom transfers initiated by Jones generally terminated in BanColombia accounts located in Colombia.

164. During this time period period, $26,503.14 was debited to Diners Club for payment of Jones' Diners Club credit card. Additional amounts were debited to pay Jones' VISA credit card.

c. Notable transactions - Port Isabel, Texas

165. Between August 14, 2013 and August 20, 2013, Jones had multiple financial transactions at various businesses located in South Padre, Texas and Port Isabel, Texas. During this same time period, known packages originating with CALIGIRL were mailed from Port Isabel, Texas. The known packages were sent via Express Mail on August 14, 2013 and August 15, 2013.

166. South Padre, Texas is approximately 5 miles from the Port Isabel, Texas U.S. Post Office. Port Isabel is approximately 550 miles from Dallas, Texas. No packages originated in or near Port Isabel outside of the above dates.

d. Notable transactions - USPS

167. Between June 14, 2013 and July 29, 2013, Jones utilized his Wells Fargo debit card to make 9 transactions with the United States Postal Service. The purchases were made at the Arlington, Texas U.S. Post Office and the Dallas, Texas U.S. Post Office. Jones spent $435 during these transactions. The average amount spent at USPS was $48.33. The highest value transactions took place on July 19, 2013 and July 29, 2013, and were both for $119.70. Jones has no known legitimate business requiring heavy use of the USPS.

B. Checking sccount xxxxxx0086 and savings sccount xxxxxx6305

168. I also reviewed records for Wells Fargo checking account xxxxxx0086 and savings account xxxxxx6305, which were opened by "J.A.L." as primary join account holder and Jones as a secondary joint account holder. The account is set up to allow either party equal access to the funds in the account. These accounts were opened, on September 26, 2013, at the Wells Fargo branch located at 11730 Preston Road, Dallas, Texas.

169. When opening accounts xxxxxx0086 and xxxxxx6305, 1861 Brown Boulevard, Box 620, Arlington, Texas was provided as the primary address for the accounts. This address corresponds to the E-Z Mail Services commercial

mail box rented by Jones. Telephone number 214-853-5236 was provided when opening the accounts. This phone number belongs to Jones.

170. Jones provided his Texas driver's license and Social Security card as forms of identification. "J.A.L." provided his Social Security card and an unknown identification card to open the account. The account opening documents stated "J.A.L." was Colombian citizen and is believed to be Jones' step-son.

a. 2013 deposits analysis of xxxxxx4421

171. For the statement periods of January 2013 through July 2013, a total of $525 was deposited into account xxxxxx4421. All of these deposits were regularly scheduled monthly transfers from Jones' checking account xxxxxx5888. All of these monthly transfers were for $75.00. In August 2013, a total of $375.00 was deposited.

172. For the statement periods of September 2013 through November 2013, a total of $22,138.55 was deposited into account xxxxxx4421. Of these deposits, $8,708.52 were either counter cash deposits or cash ATM deposits, one check was deposited in the amount of $1,904.44, one online transfer of $3,800 was made from Jones' checking account xxxxxx5888, and $7,500 was deposited from Jones' Wells Fargo line of credit.

b. 2013 debits analysis of xxxxxx4421

173. For the statement periods of January 2013 through August 2013, a total of $360 was debited from account xxxxxx4421. During the statement

periods of September through October 2013 a total of $12,720.50 was debited from account xxxxxx4421. Of these debits, $5,000 was transferred to Jones' personal line of credit and $7,720.50 was transferred to Jones' checking account xxxxxx5888).

c. *2013 credits analysis of xxxxxx6305*

174. Account xxxxxx6305 was opened in September 2013. Between September 2013 and November 2013, the account received cash counter-deposits totaling $7,680.07. One additional deposit, totaling $100.00, was made when the account was opened. The average value of cash deposits was $768. The counter-deposits appeared to have been made from multiple Wells Fargo Branch locations. The deposit slips contained only the minimum amount of information required to make a cash deposit. Based on my training and experience, this is common behavior utilized by Bitcoin exchangers and drug traffickers utilizing counter deposits to transmit currency.

d. *2013 debits analysis of xxxxxx6305*

175. Between September 2013 and November 2013, debits totaling $5,570.06 were made from account xxxxxx6305. Of these, $2,500 was transferred to Jones' checking account xxxxxx5888, $1,152.49 was transferred to Jones' VISA credit card accounts, and $1,899.33 was transferred to Jones' Wells Fargo line of credit. The account did not indicate any living expense debits, such as rent or utilities.

C. Account xxxxxx0086

a. 2013 credits analysis of xxxxxx0086

176. During statement period of October 2013 through November 2013, $3,696.45 was credited to xxxxxx0086. Of these deposits, $3,696.45 were cash counter deposits. An initial account opening deposit of $100.00 was also deposited. The average deposit was $759.40. The counter deposits appeared to have been made at multiple Wells Fargo Branch locations. The deposit slips contained only the minimum amount of information required to make a cash deposit. Based on my training and experience, this is a common behavior utilized by Bitcoin exchangers and drug traffickers utilizing to transmit currency.

b. 2013 debits analysis of xxxxxx0086

177. Between October 2013 through November 2013, $960 was debited from the account. The debit was transferred to Jones' checking account, xxxxxx5888.

JP Morgan Chase Bank

178. As part of my investigation, I reviewed financial records obtained from JP Morgan Chase ("JPMC") regarding accounts held at that institution by Jones for JPMC account xxxxxx9730. The account was opened on December 7, 2009 by Jones, who provided his Texas driver's license as a form of identification when opening the account. The account was opened at the Downtown Dallas, Texas branch of Chase Bank, 2200 Ross Avenue, Dallas, Texas. 2200 Ross

Ave, Dallas, Texas was the return address printed on at least 8 packages that originated with CALIGIRL, including the October 22, 2013 undercover purchase.

179. When opening the account, Jones used his E-Z Mail Servies mailbox as the primary address.

180. The records that I reviewed covered the time period of January 17, 2013 through January 17, 2014.

a. *Deposits analysis*

181. Between January 2013 and May 2013, a total of $1,349.16 was deposited into account xxxxxx9730. None of these deposits were cash deposits, nor were any made at bank branch locations. The deposits were regularly scheduled transfers from additional bank accounts controlled by Jones.

182. Between June 2013 and January 2014, $47,012.98 was deposited into account xxxxxx9730. During this period, $22,035 of cash was deposited into the account. Included in the cash deposits were numerous deposits made at bank branch counters. Account xxxxxx9730 also received one check deposit of $19,300.33. The memo reference for this deposit was "Loan Repayment." During this period, the account received $1,991.06 from Dwolla.

b. *Debits analysis*

183. Between January 2013 and May 2013, $832.75 was debited from xxxxxx9730. These debits appeared to be regularly scheduled direct debits and payments for a Chase credit card.

184. Between June 2013 and January 2014, $42,630.06 was debited from account xxxxxx9730. Of those debits, $2,002.99 was debited by Xoom, $1,571 was withdrawn at ATMs located in Colombia, and $8,246.84 was debited to pay for Jones' Diners Club credit card. An additional $4,750.19 was debited to pay Jones' Chase VISA. Jones also wrote a check for $13,100 for advanced payment of rent through June 2014 for 13625 Far Hills Lane, Dallas, Texas.

c. *Notable Transactions*

185. On August 15, 2013, Jones utilized the debit card associated with account xxxxxx9730 to make a $23.66 purchase and a $404 ATM withdrawal at a Walmart in Port Isabel, Texas. During this same time period, known packages originating with CALIGIRL were mailed from Port Isabel, Texas. These packages were sent using Express Mail on August 14, 2013 and August 15, 2013.

186. On July 9, 2013, Jones utilized the Chase debit card associated with account xxxxxx9730 to make a $117.85 purchase at the United States Post Office in Dallas, Texas.

Western Union Wire Transfers

187. As part of this investigation, I reviewed records received from Western Union relating to Jones' use of its wire transfer services. The records covered the time period of September 21, 2013 through October 9, 2013.

188. Between September 22, 2013 and October 9, 2013, Jones received 53 Western Union wire transfers totaling $33,404.23. The wire transfers were initiated by multiple subjects and originated in different geographical

locations. The originating locations included 16 different states, Mexico, Chile, Germany, and Sweden.

189. Of the 53 identified transactions, the average amount received by Jones was $630.26. The largest single transaction during this time period was $1,047.92 and was received by Jones on October 6, 2013. The smallest single transaction identified was $209 and was received by Jones on September 21, 2013.

190. Jones provided the following addresses to Western Union when receiving funds:

- 2755 Fairview, Grand Prairie, TX 75050
- 2755 Fairway Park, Grand Prairie, TX 75050
- 2722 Fairway Park, Fort Worth, TX 75050
- 12009 Coit Road, Dallas, TX 75251

191. Jones provided the following telephone numbers to Western Union:

- 214-853-5236
- 214-853-5276
- 214-853-5536
- 214-853-2636
- 214-853-5230
- 214-853-5296
- 214-857-8236

192. Based on my training and experience, I know that small variations in telephone numbers, addresses and other identifying information is a common method drug traffickers and money launderers utilize to avoid detection by law enforcement.

193. Jones provided his Texas driver's license number when receiving funds from Western Union.

194. Wire transfers received by Jones were generally picked up at a Western Union agent location within two hours of the funds being sent; however, some proceeds were picked up in less than one hour.

195. Jones used various Western Union locations throughout the Dallas metropolitan area to pick up currency. Based on my training and experience, this is a common method drug traffickers and money launderers utilize to avoid detection by not establishing a pattern or any regularity of actions. Utilizing multiple locations also prevents employees of the establishments from becoming familiar with those utilizing the wire transfer service.

From my review of the wire transfers, there did not appear to be a consistent relationship between individuals sending funds. The wire transfers were initiated in a variety geographic locations. Additionally, there did not appear to be a familial or business relationship between the currency senders and Jones as the individuals sending the wire transfers utilized their personal names and not any official or corporate identities.

MoneyGram Wire Transfers

196. As part of my investigation, I reviewed Jones' use of MoneyGram wire transfer services. The records reviewed include transactions dated between September 28, 2013 and October 8, 2013. When he opened his account, Jones provided his name, listed his address as 2755 Fairway Park St., Grand Prairie, Texas and provided his Texas driver's license as proof of identity.

197. Between September 28, 2013 and October 8, 2013, Jones received 23 MoneyGram wire transfers, totaling $12,872.22. The wire transfers were initiated by multiple individuals and originated in different geographical locations including 13 different States and Brazil. Of the 23 transactions, the average dollar amount received by Jones was $559.66. The largest single transaction was $899 and was received by Jones on October 5, 2013. The smallest transactions received by Jones were for $450. Jones received nine $450.00 wire transfers during the period, all of which originated with different individuals.

198. Wire transfers received by Jones were generally picked up from a MoneyGram agent within several hours of being sent and some wire transfers were picked up within one hour of being sent.

199. Jones used various MoneyGram agent locations throughout the Dallas metropolitan area.

200. From my review of the transactions, there was not a consistent relationship between the individuals sending funds and Jones. The wire transfers were initiated in various geographic locations. Additionally, there did

not appear to be a familial or business relationship between those sending currency and Jones. The individuals sending wire transfers utilized personal names and not official or corporate identities.

Jones' Accounts on http://localbitcoins.com and http://bitcoin-otc.com

201. In addition Jones utilizing Western Union to exchange Bitcoins into U.S. currency, Jones offered Bitcoins for sale in exchange for cash deposited directly into bank accounts he controlled. To accomplish this, Jones was a Bitcoin exchange vendor on both http://localbitcoins.com (LBC) and http://bitcoin-otc.com (BTC-OTC). These websites offer anonymous Bitcoin currency exchanges.

202. LBC provided a profile page to each vendor and it was utilized as a space for a vendor to adverse his or her trade offers and prices. The user is afforded a small space in which to place a message which may be related to their trade policies. LBC profile pages list some feedback a user has received and maintains a record of up to 100 transactions undertaken.

203. Jones operated on LBC under the pseudonym "Dynamite2k". Through his LBC profile, I was able to determine that Jones utilized LBC to make over 100 Bitcoin trades, with 97 unique partners. Jones received 100% positive feedback.[46] Jones' LBC profile was deleted on or about March 17, 2014 and was previously located at http://localbitcoins.com/p/dynamite2k.

[46] Positive feedback is provided to a LBC vendor upon completion of a successful trade.

204. Through Jones' LBC profile, I was able to determine that Jones offered Bitcoins for sale in exchange for U.S. dollars. Jones accepted trades that were made through Western Union and cash in person. Additionally, Jones offered Bitcoins for sale through bank counter deposits made at Wells Fargo bank or Chase Bank.[47]

205. Jones' LBC profile indicated that he would process cash in person for exchanges in the Dallas, Texas area.

206. Jones also maintained an account on http://bitcoin-otc.com ("BTC-OTC") under the pseudonym "Dynamite`." This account was linked to LBC by the software operating BTC-OTC and in order to encourage trust by showing "Dynamite`" and "Dynamite2k" were the same person.

207. BTC-OTC does not provide information regarding the numbers of past trades, however it does show some feedback. BTC-OTC also links feedback to LB, showing a user's LBC feedback on their BTC-OTC profile.

208. Throughout this investigation, I discovered a large amount of information indicating Jones was high volume Bitcoin seller. Through his business of selling controlled substances in exchange for Bitcoin, Jones acquired large numbers of Bitcoins and utilized websites such as LBC and BTC-OTC to exchange the criminal proceeds in to U.S. dollars.

---

[47] During a bank counter deposit, the vendor provides the purchaser with a bank account number, institution and account holder name. The purchaser physically goes to a branch of the named financial institution and makes a cash deposit in to the provided bank account. This is a method heavily utilized by Bitcoin traders.

209. The activity, as detailed in this affidavit, reveals that Jones received large numbers of incoming consumer remittance wire transfers[48] and anonymous bank counter deposits[49] which are consistent with exchanging Bitcoin for U.S. currency. Based upon my training, experience, and my review of the above accounts, the activity taking place in all of the accounts is consistent with Jones operating a Bitcoin exchange for drug trafficking and money laundering activity.

Conclusion

210. Based on the information set forth herein, I submit that there is probable cause to believe that Matthew Jones, a/k/a "CALIGIRL," a/k/a "Dynamite2k" a/k/a "Dynamite`," a/k/a "Tyler Zeddai," a/k/a "Mateo Jones" has violated 21 U.S.C. §§ 841(a)(1) and 841(b)(1)(C) (distribution of a controlled substance).

211. This concludes my affidavit.

Jared Gabbay
Task Force Agent
Drug Enforcement Administration

Sworn to and subscribed before me
this 14th day of May, 2014

The Honorable Gregory J. Kelly
UNITES STATES MAGISTRATE JUDGE

48 Western Union and MoneyGram are consumer wire transfer remitters.

49 Persons undertaking bank counter deposits are generally instructed to only provide the required information (account number and account holder name) when making a deposit, even though the deposit slips have space for more information. They are also instructed to not answer any questions asked by the bank teller servicing the deposit.

Exhibit 1

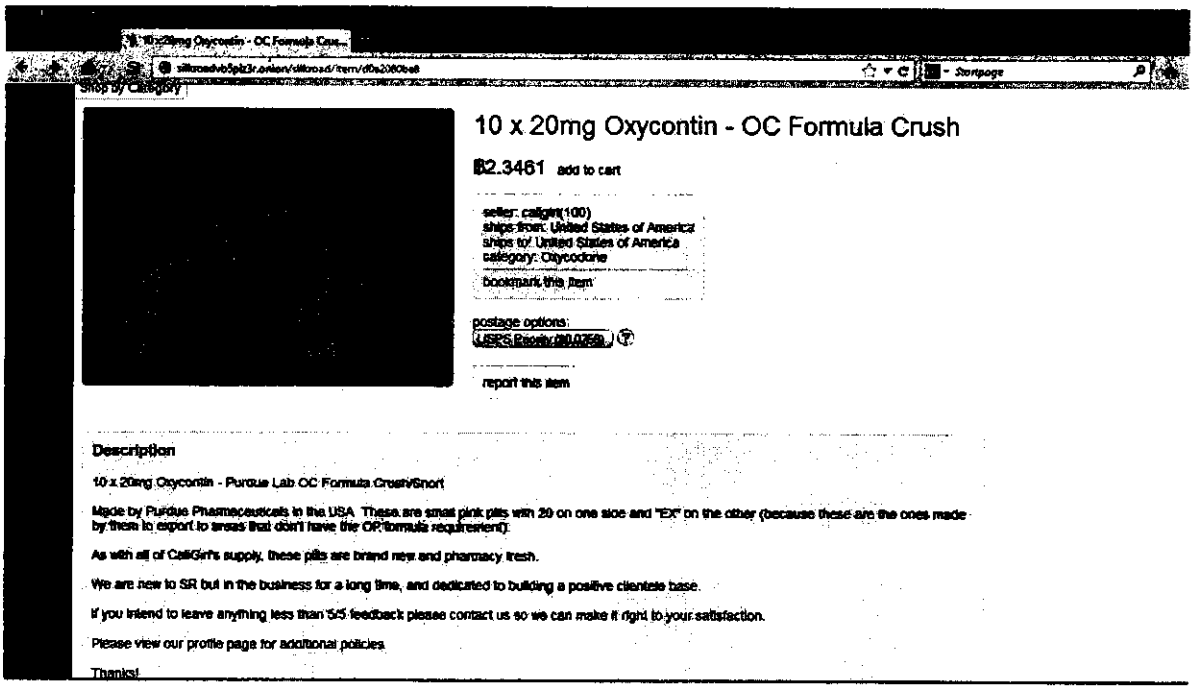
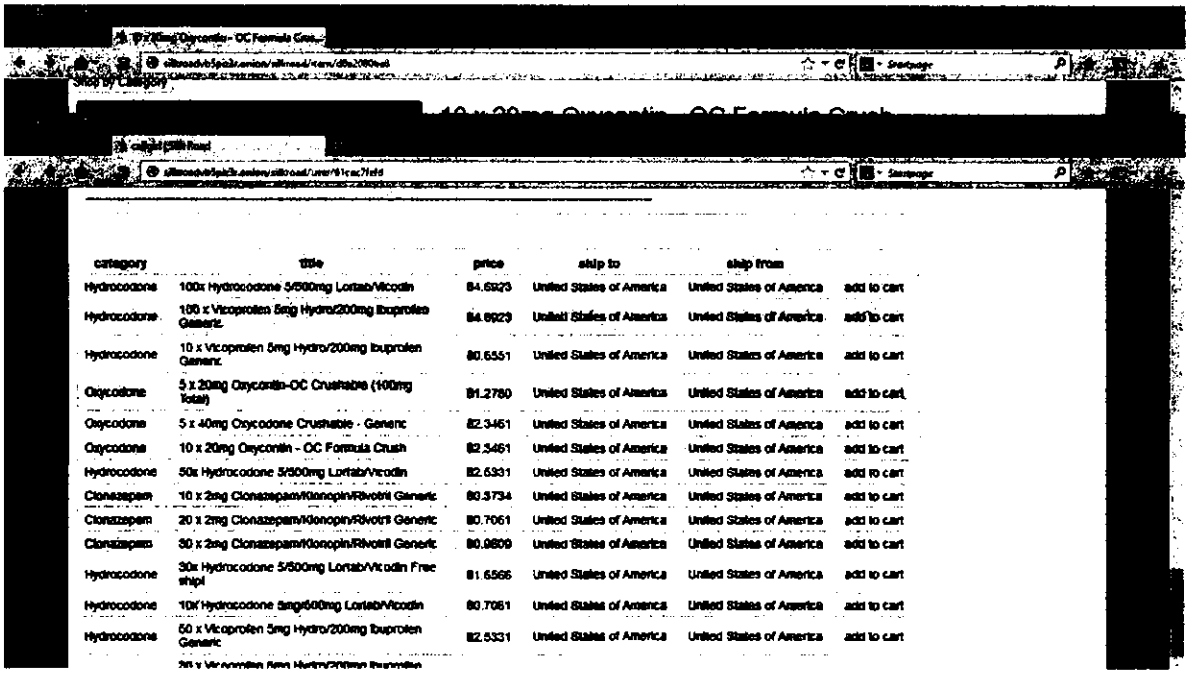

10 x 20mg Oxycontin - OC Formula Crush
Ƀ2.3461 add to cart
seller: caligirl(100)
ships from: United States of America
ships to: United States of America
category: Oxycodone
bookmark this item
postage options:
report this item
Description
10 x 20mg Oxycontin - Purdue Lab OC Formula Crush/Snort
Made by Purdue Pharmaceuticals in the USA. These are small pink pills with 20 on one side and "EX" on the other (because these are the ones made by them to export to areas that don't have the OP formula requirement).
As with all of CaliGirl's supply, these pills are brand new and pharmacy fresh.
We are new to SR but in the business for a long time, and dedicated to building a positive clientele base.
If you intend to leave anything less than 5/5 feedback please contact us so we can make it right to your satisfaction.
Please view our profile page for additional policies.
Thanks!

Exhibit 2



category	title	price	ship to	ship from	
Hydrocodone	100x Hydrocodone 5/500mg Lortab/Vicodin	84.6923	United States of America	United States of America	add to cart
Hydrocodone	100 x Vicoprofen 5mg Hydro/200mg Ibuprofen Generic	84.6923	United States of America	United States of America	add to cart
Hydrocodone	10 x Vicoprofen 5mg Hydro/200mg Ibuprofen Generic	80.6551	United States of America	United States of America	add to cart
Oxycodone	5 x 20mg Oxycontin-OC Crushable (100mg Total)	81.2780	United States of America	United States of America	add to cart
Oxycodone	5 x 40mg Oxycodone Crushable - Generic	82.3461	United States of America	United States of America	add to cart
Oxycodone	10 x 20mg Oxycontin - OC Formula Crush	82.3461	United States of America	United States of America	add to cart
Hydrocodone	50x Hydrocodone 5/500mg Lortab/Vicodin	82.5331	United States of America	United States of America	add to cart
Clonazepam	10 x 2mg Clonazepam/Klonopin/Rivotril Generic	80.3734	United States of America	United States of America	add to cart
Clonazepam	20 x 2mg Clonazepam/Klonopin/Rivotril Generic	80.7061	United States of America	United States of America	add to cart
Clonazepam	50 x 2mg Clonazepam/Klonopin/Rivotril Generic	80.9809	United States of America	United States of America	add to cart
Hydrocodone	30x Hydrocodone 5/500mg Lortab/Vicodin Free shipl	81.6566	United States of America	United States of America	add to cart
Hydrocodone	10X Hydrocodone 5mg/500mg Lortab/Vicodin	80.7061	United States of America	United States of America	add to cart
Hydrocodone	50 x Vicoprofen 5mg Hydro/200mg Ibuprofen Generic	82.5331	United States of America	United States of America	add to cart

Exhibit 3-A

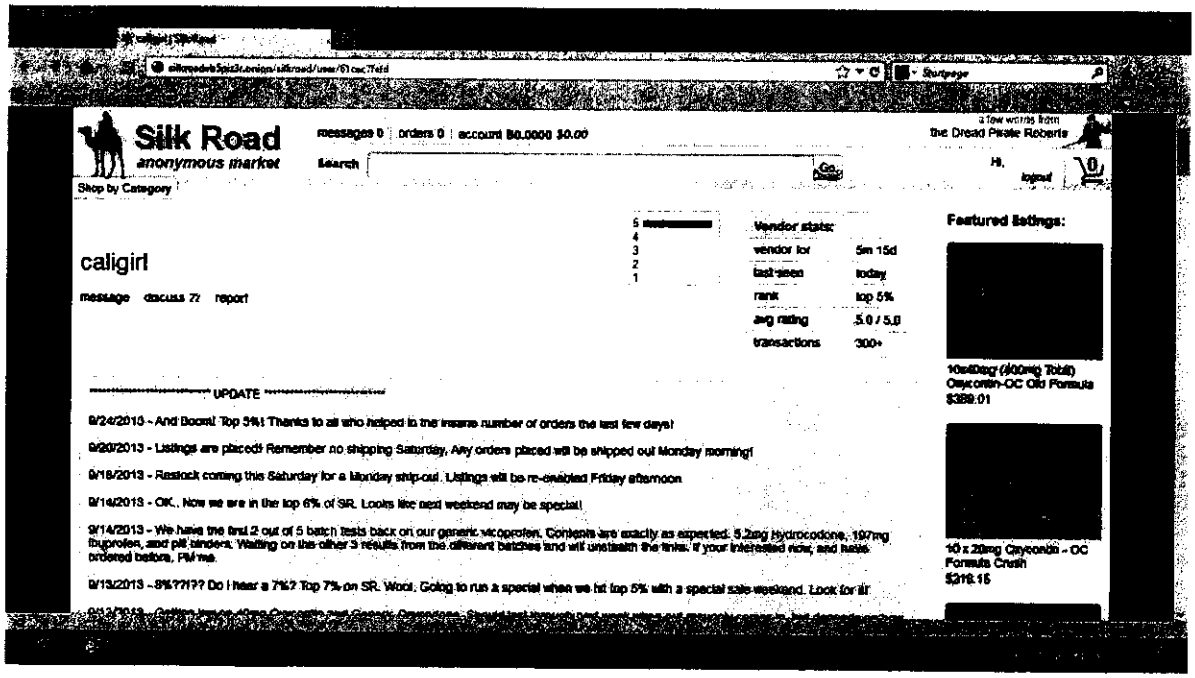
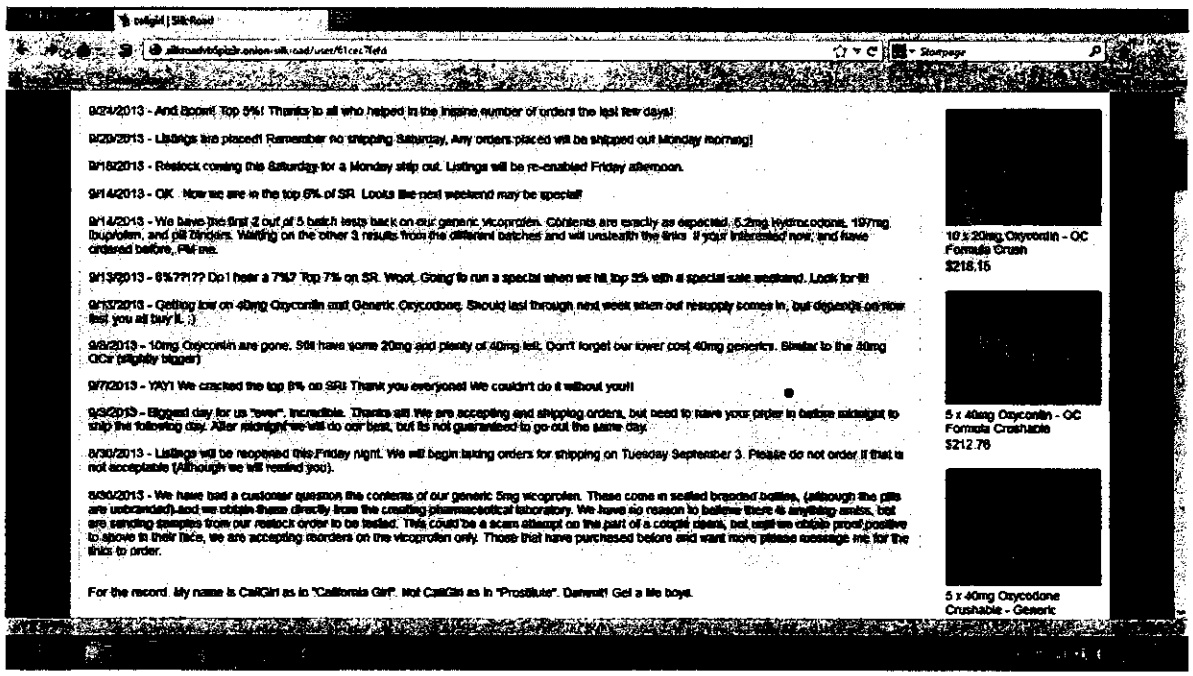

Silk Road
anonymous market
Shop by Category
messages 0 | orders 0 | account $0.0000 $0.00
Search
a few words from
the Dread Pirate Roberts
Hi,
logout
caligirl
message discuss 77 report
Vendor stats:
vendor for 5m 15d
last seen today
rank top 5%
avg rating 5.0 / 5.0
transactions 300+
Featured listings:
10x80mg (800mg Total)
Oxycontin-OC Old Formula
$389.01
10 x 20mg Oxycontin - OC
Formula Crush
$219.15
UPDATE
9/24/2013 - And Boom! Top 5%! Thanks to all who helped in the insane number of orders the last few days!
9/20/2013 - Listings are placed! Remember no shipping Saturday. Any orders placed will be shipped out Monday morning!
9/18/2013 - Restock coming this Saturday for a Monday ship-out. Listings will be re-enabled Friday afternoon.
9/14/2013 - OK, Now we are in the top 6% of SR. Looks like next weekend may be special!
9/14/2013 - We have the first 2 out of 5 batch tests back on our generic vicoprofen. Contents are exactly as expected. 5.2mg hydrocodone, 197mg
ibuprofen, and pill binders. Waiting on the other 3 results from the different batches and will unstealth the links if your interested now, see feats
ordered before, PM me.
9/13/2013 - 8%??!?? Do I hear a 7%? Top 7% on SR. Woot. Going to run a special when we hit top 5% with a special sale weekend. Look for it!

Exhibit 3-B



9/24/2013 - And Boom! Top 5%! Thanks to all who helped in the insane number of orders the last few days!

9/20/2013 - Listings are placed! Remember no shipping Saturday. Any orders placed will be shipped out Monday morning!

9/18/2013 - Restock coming this Saturday for a Monday ship out. Listings will be re-enabled Friday afternoon.

9/14/2013 - OK. Now we are in the top 6% of SR. Looks like next weekend may be special!

9/14/2013 - We have the first 2 out of 5 batch tests back on our generic vicoprofen. Contents are exactly as expected. 5.2mg hydrocodone, 197mg ibuprofen, and pill binders. Waiting on the other 3 results from the different batches and will unleash the links. If your interested now, and have ordered before, PM me.

9/13/2013 - 6%??!!? Do I hear a 7%? Top 7% on SR. Woot. Going to run a special when we hit top 5% with a special sale weekend. Look for it!

9/12/2013 - Getting low on 40mg Oxycontin and Generic Oxycodone. Should last through next week when our resupply comes in, but depends on how fast you all buy it. :)

9/9/2013 - 10mg Oxycontin are gone. Still have some 20mg and plenty of 40mg left. Don't forget our lower cost 40mg generics. Similar to the 40mg OCs (slightly bigger)

9/7/2013 - YAY! We cracked the top 8% on SR! Thank you everyone! We couldn't do it without you!!

9/3/2013 - Biggest day for us *ever*. Incredible. Thanks all! We are accepting and shipping orders, but need to have your order in before midnight to ship the following day. After midnight we will do our best, but its not guaranteed to go out the same day.

8/30/2013 - Listings will be reopened this Friday night. We will begin taking orders for shipping on Tuesday September 3. Please do not order if that is not acceptable (Although we will refund you).

8/30/2013 - We have had a customer question the contents of our generic 5mg vicoprofen. These come in sealed branded bottles, (although the pills are unbranded)-and we obtain these directly from the creating pharmaceutical laboratory. We have no reason to believe there is anything amiss, but are sending samples from our restock order to be tested. This could be a scam attempt on the part of a couple users, but until we obtain proof positive to above in their face, we are accepting reorders on the vicoprofen only. Those that have purchased before and want more please message me for the links to order.

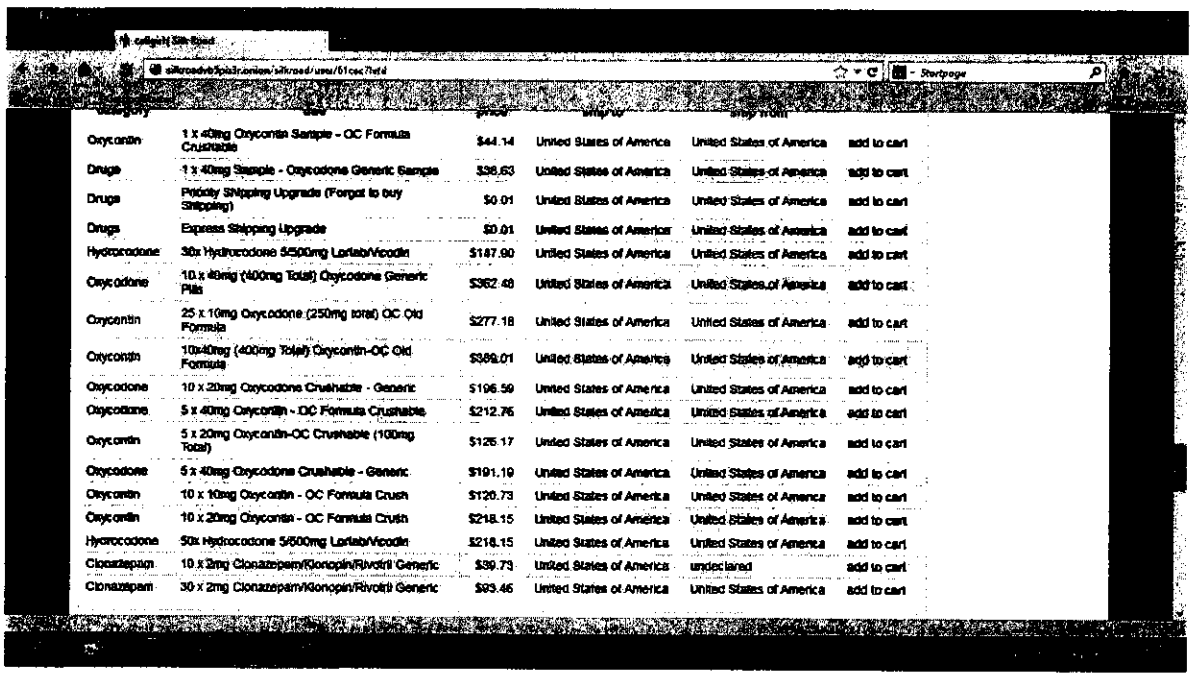
For the record. My name is CalGirl as in "California Girl". Not CalGirl as in "Prostitute". Damnit! Get a life boys.

10 x 20mg Oxycontin - OC Formula Crush
$218.15

5 x 40mg Oxycontin - OC Formula Crushable
$212.76

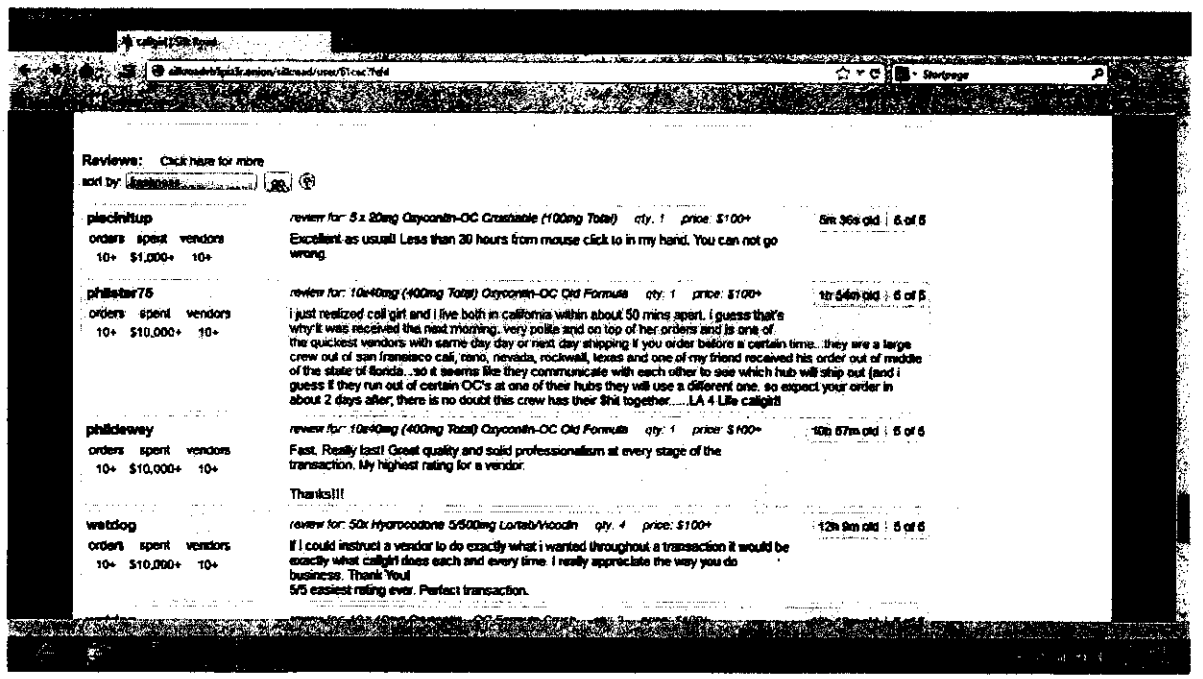
5 x 40mg Oxycodone Crushable - Generic

Exhibit 3-C



Oxycontin	1 x 40mg Oxycontin Sample - OC Formula Crushable	$44.14	United States of America	United States of America	add to cart
Drugs	1 x 40mg Sample - Oxycodone Generic Sample	$36.63	United States of America	United States of America	add to cart
Drugs	Priority Shipping Upgrade (Forgot to buy Shipping)	$0.01	United States of America	United States of America	add to cart
Drugs	Express Shipping Upgrade	$0.01	United States of America	United States of America	add to cart
Hydrocodone	30x Hydrocodone 5/500mg Lorlab/Vicodin	$187.90	United States of America	United States of America	add to cart
Oxycodone	10 x 40mg (400mg Total) Oxycodone Generic Pills	$362.48	United States of America	United States of America	add to cart
Oxycontin	25 x 10mg Oxycodone (250mg total) OC Old Formula	$277.18	United States of America	United States of America	add to cart
Oxycontin	10x40mg (400mg Total) Oxycontin-OC Old Formula	$389.01	United States of America	United States of America	add to cart
Oxycodone	10 x 20mg Oxycodone Crushable - Generic	$196.59	United States of America	United States of America	add to cart
Oxycodone	5 x 40mg Oxycontin - OC Formula Crushable	$212.76	United States of America	United States of America	add to cart
Oxycontin	5 x 20mg Oxycontin-OC Crushable (100mg Total)	$126.17	United States of America	United States of America	add to cart
Oxycodone	5 x 40mg Oxycodone Crushable - Generic	$191.19	United States of America	United States of America	add to cart
Oxycontin	10 x 10mg Oxycontin - OC Formula Crush	$120.73	United States of America	United States of America	add to cart
Oxycontin	10 x 20mg Oxycontin - OC Formula Crush	$218.15	United States of America	United States of America	add to cart
Hydrocodone	50x Hydrocodone 5/500mg Lorlab/Vicodin	$218.15	United States of America	United States of America	add to cart
Clonazepam	10 x 2mg Clonazepam/Klonopin/Rivotril Generic	$39.73	United States of America	undeclared	add to cart
Clonazepam	30 x 2mg Clonazepam/Klonopin/Rivotril Generic	$93.46	United States of America	United States of America	add to cart

Exhibit 3-D



Reviews: Click here for more

sort by: [redacted] go

placinitup
orders spent vendors
10+ $1,000+ 10+

review for: 5 x 20mg Oxycontin-OC Crushable (100mg Total) qty: 1 price: $100+ — 5m 36s old | 6 of 6

Excellent as usual! Less than 30 hours from mouse click to in my hand. You can not go wrong.

philster75
orders spent vendors
10+ $10,000+ 10+

review for: 10x40mg (400mg Total) Oxycontin-OC Old Formula qty: 1 price: $100+ — 1hr 54m old | 6 of 6

i just realized coil girl and i live both in california within about 50 mins apart. i guess that's why it was received the next morning. very polite and on top of her orders and is one of the quickest vendors with same day day or next day shipping if you order before a certain time...they are a large crew out of san fransisco cali, reno, nevada, rockwall, texas and one of my friend received his order out of middle of the state of florida...so it seems like they communicate with each other to see which hub will ship out (and i guess if they run out of certain OC's at one of their hubs they will use a different one. so expect your order in about 2 days after, there is no doubt this crew has their $hit together.....LA 4 Life caligirl!

philidewey
orders spent vendors
10+ $10,000+ 10+

review for: 10x40mg (400mg Total) Oxycontin-OC Old Formula qty: 1 price: $100+ — 10h 57m old | 6 of 6

Fast. Really fast! Great quality and solid professionalism at every stage of the transaction. My highest rating for a vendor.

Thanks!!!

wetdog
orders spent vendors
10+ $10,000+ 10+

review for: 50x Hydrocodone 5/500mg Lortab/Vicodin qty: 4 price: $100+ — 12h 9m old | 5 of 5

If I could instruct a vendor to do exactly what i wanted throughout a transaction it would be exactly what caligirl does each and every time. I really appreciate the way you do business. Thank You!
5/5 easiest rating ever. Perfect transaction.

Exhibit 4