

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America

v.

OLIVIA LOUISE BOLLES
a/k/a "MDPRO"

Case No.

6:13-mj-1614

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of 06/13/2013 to 08/20/2013 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 (b)(1)(C)

Distribution of a mixture and substance containing a detectable amount of a controlled substance.

This criminal complaint is based on these facts:

☒ Continued on the attached sheet.*Complainant's signature*

Jarad Gabbay, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

11/19/2013*Judge's signature*

City and state:

Orlando, FL

David A. Baker, Magistrate Judge

Printed name and title

**STATE OF FLORIDA
COUNTY OF ORANGE**

6:13-mj-1614

AFFIDAVIT

I, Jared F. Gabbay, being duly sworn, do 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 narcotic investigators, supervisors, and prosecutors, and have

conducted extensive investigations of organized criminal racketeering offenses and narcotic crimes, including the use of visual surveillance, electronic surveillance, informant interviews, interrogation, and undercover operations. In connection with drug trafficking investigations, I have participated in and/or executed numerous search warrants, including 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, information from confidential sources, financial institutions, other business entities, as well as other documents and records obtained by law enforcement during the course of this investigation. 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

5. This affidavit is submitted in support of a criminal complaint and arrest warrant for **Olivia Louise BOLLES a/k/a "MDPRO"** for violations of 21 U.S.C. §§ 841(a)(1) and 841(b)(1)(C) (distribution of a controlled substance).

Structure of this Affidavit

6. This affidavit is divided into separate sections to present the information herein to the Court. First, I provide "Summary of the Investigation" which gives an overview of the investigation and evidence which is subject of this affidavit. Second, I provide a "Subject of this Investigation" section. Third, I provide a "Background on Silk Road" in which I explain the Silk Road drug marketplace 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 "MDPRO," describe a "Feedback Based Sales Analysis of MDPRO," and outline an "Analysis of Postal Information of Packages Sent by MDPRO." Furthermore, I detail "Undercover Purchases of Controlled Substances from MDPRO" and I describe how I identified **BOLLES** as MDPRO. Next, I detail a "Financial Records Analysis." In the fifth section of the affidavit, titled "14 Sunny Bend, Newark, Delaware 19701," I detail evidence relating to **BOLLES'** residence. In the sixth section, I describe "IP Addresses Utilized by **BOLLES.**"

Summary of the Investigation

7. The investigation determined that **BOLLES**, a licensed medical doctor, illegally sold controlled substances on the Silk Road drug marketplace website using the alias "MDPRO."

8. As part of the investigation, on the Silk Road website, I made several undercover purchases of controlled substances from "MDPRO." From reviewing bank and business records, the investigation confirmed that **BOLLES** utilized the Silk Road alias "MDPRO." The investigation established that **BOLLES** was the person who shipped the controlled substances that were purchased from MDPRO. The investigation determined that **BOLLES** utilized her personal bank accounts to purchase items which were later utilized to further her illegal drug dealing business, including packaging materials and laboratory materials.

9. On the Silk Road website, **BOLLES** offered to sell controlled substances which, once purchased, were delivered to customers using the United States Postal Service (USPS). The investigation identified more than 600 sales of controlled substances that were mailed by **BOLLES** to individuals in more than 17 different countries.

Subject of the Investigation

10. **Olivia Louise BOLLES a/k/a "MDPRO"** attended the University of Missouri-Columbia School of Medicine where she obtained her medical doctorate. Prior to attending medical school, **BOLLES** held a State of Missouri

pharmacy technician license. **BOLLES** is currently a licensed medical doctor in the State of Delaware with license number C1-0010699. **BOLLES** is currently listed on the Christiana Care Health System website¹ as a fourth year resident/chief resident of obstetrics and gynecology.

11. **BOLLES** does not presently hold a controlled substance dispensing license, nor does she have a DEA Registration Number. **BOLLES** has a controlled substance license application pending in the State of Delaware.

12. While practicing as a licensed doctor, **BOLLES** operated a vendor account on the Silk Road drug marketplace using the alias MDPRO.

13. **BOLLES'** home address is 14 Sunny Bend, Newark, Delaware, 19702.

Background of Silk Road

14. 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

¹ <http://www.christianacare.org/residentlist>

on the network, and, as a result, the identities of the network's users.² 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>.³

15. 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.

² 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.

³ 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.

16. 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.

17. 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.

18. 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."

19. 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

20. 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 and other controlled substances of nearly every variety, which were openly advertised on the website and prominently visible on the website's home page.

21. 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" or "80mg Oxycodone (OP80) - \$50 each" or "QUALITY #4 HEROIN ALL ROCK."

22. 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.

23. 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 drivers 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.

24. 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."

25. 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

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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 vendor’s 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.

Probable Cause

Background of Silk Road Vendor “MDPRO”

36. Based upon my knowledge of the Silk Road website and through this investigation, I became familiar with a drug vendor who operated on the Silk Road under the username “MDPRO.” MDPRO opened a vendor account on Silk Road in or about March 2013. Silk Road vendors were provided with a personal webspace 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 MDPRO's offerings, as of July 26, 2013, is attached to this affidavit as Exhibit 2.

37. MDPRO offered various pharmaceutical controlled substances for sale including, Oxycodone⁴, Mixed Amphetamine Salts (Adderall)⁵, and Alprazolam⁶. Additionally, MDPRO offered to sell items of “Butane Hash Oil” (BHO) which is a concentrated Tetrahydrocannabinol⁷ (THC). Based upon my training, experience, and this investigation, I know that the BHO production process involves a very high risk of injury or death due to the flammability of the fuel utilized to produce the BHO.

⁴ Oxycodone is a Schedule II controlled substance.

⁵ Mixed Amphetamine Salts (Adderall) are a Schedule II controlled substance.

⁶ Alprazolam is a Schedule IV controlled substance.

⁷ Tetrahydrocannabinol is a Schedule I controlled substance.

38. MDPRO also offered a "Physician Consultation" service for sale on its Silk Road vendor page. The listing stated that a purchaser would obtain "email access to a U.S. licensed physician for general medical questions, symptom management, and assistance with how to get what you want or need when being seen in a doctor's office...He will not prescribe medications, but will advise you on how to obtain them."

39. MDPRO made several postings on the Silk Road Forum. Based on my training, experience, and this investigation, I believe these postings showed that MDPRO had advanced training in medicine and pharmacy. Specifically, on June 2, 2013, MDPRO posted information on the Silk Road forum information about "Heroin Arterial Injection" wherein MDPRO provided advice on giving heroin injections. Also, on June 2, 2013, MDPRO posted on the Silk Road forum in a conversation regarding Actavis Syrup.⁸ MDPRO stated that she was going to manufacture a homemade version of pharmaceutical Actavis Syrup for distribution on Silk Road. MDPRO stated the concentrations of medications would be the same as the commercial product. MDPRO claimed to have precise equipment and a background in pharmacy, including compounding.⁹

Feedback Based Sales Analysis of MDPRO

40. On or about July 29, 2013, I performed an analysis of the feedback posted on MDPRO's Silk Road vendor page. The feedback was left by

⁸ Actavis Syrup is a cough syrup containing codeine, a Schedule II controlled substance.

⁹ Pharmaceutical compounding is the precise mixing of medications to create a specific medication upon the order of a physician.

previous customers of MDPRO and listed each product the feedback was in response to and the approximate age of the feedback. A user was not compelled to leave feedback for a transaction, nor could a user leave multiple items of feedback for a single order. Consequently, the analysis represented the minimum number of transactions in which MDPRO undertook as a vendor on Silk Road and was not representative of all transactions where MDPRO was the selling party.

41. In my analysis of MDPRO's feedback, I located 610 drug transactions between MDPRO and Silk Road users. The users were not identified in the feedback. The transactions included MDPRO's sale of:¹⁰

- Diazepam¹¹ 15mg: 675 tablets
- E-Cigarette Cartridges containing THC⁵: 49 lots¹²
- Flunitrazepam¹³ 2mg: 38 tablets
- Phentermine¹⁴ 37.5mg: 335 tablets
- Phentermine 50mg: 90 tablets
- Alprazolam⁴ 2mg: 540 tablets
- Alprazolam⁴ 1mg: 40 tablets
- Adderall³ 30mg: 245 tablets
- Adderall³ 5mg: 30 tablets
- Oxycodone²: 40mg: 12 tablets
- Oxycodone² 30mg: 12 tablets
- Lisdexamfetamine¹⁵ 60mg: 65 tablets
- Codeine¹⁶ Syrup 4oz: 17 lots (68 fluid ounces)

¹⁰ The list does not account for any transactions occurring on or after July 29, 2013.

¹¹ Diazepam is a Schedule IV controlled substance.

¹² A "lot" on the Silk Road Website is terminology for a single advertisement that offers a specific quantity of an item, or a grouping of items.

¹³ Flunitrazepam (Rohypnol) is a Schedule IV controlled substance.

¹⁴ Phentermine is a Schedule IV controlled substance

¹⁵ Lisdexamfetamine (Vyance) is a Schedule II controlled substance.

¹⁶ Codeine is a Schedule II controlled substance.

- Codeine Syrup (unknown size): 10 lots
- Hydrocodone/Acetaminophen¹⁷ 10/325mg: 25 tablets
- Hydrocodone/Acetaminophen¹² 5/325mg: 20 tablets
- Testosterone Gel¹⁸ (unknown size): 3 lots (unknown quantity per lot)

42. Silk Road vendors were able to place "Custom Listings" for sale on their vendor page for users that requested a specific product or specific amounts. Feedback may appear for these products, however, the actual item sold was not displayed.

Analysis of Postal Information of Packages Sent by MDPRO

43. I obtained records from the United States Postal Inspection Service (USPIS) regarding a USPS account utilized by MDPRO. As further detailed in this affidavit, I subsequently identified MDPRO's USPS account as being opened and operated by **Olivia BOLLES**.

44. Between June 17, 2013 and August 7, 2013, **BOLLES'** USPS account was used to send 368 unique packages to 332 unique locations in 17 countries. Of those, 42 packages were destined for locations outside of the United States. Included in the list of outbound packages were two undercover purchases I made from MDPRO using Silk Road. Also included on the USPS list was a package which was destined for a person in Australia. The package was seized by Australian Customs on July 1, 2013 and, after it was searched, was

¹⁷ Hydrocodone is a Schedule III controlled substance, when in combination with Acetaminophen.

¹⁸ Testosterone gel is a Schedule III controlled substance.

found to contain 250 Alprazolam 2mg tablets concealed in "Johnson & Johnson" brand first aid kits.

45. All of the packages detailed by the USPS listed a return address of "Samples Unlimited, 26 Fox Hunt Lane PMB 176, Bear, DE 19701." This address is a commercial Post Office Box that was rented by **BOLLES**. **BOLLES** utilized her personal e-mail address, Olivia **BOLLES**@yahoo.com, to open the USPS account. With the exception of two packages, all of the postage was paid with **BOLLES'** personal VISA card or **BOLLES'** personal PayPal account.

46. Additional records supplied by the USPS for packages sent between August 22, 2013 and September 10, 2013 showed that **BOLLES'** account was used to send an additional 42 unique packages to destinations in six countries. Three packages were sent listing the return addresses of 14 Sunny Bend, Newark, Delaware 19702. The remaining 39 packages were sent with a return address of "Samples Unlimited, 26 Fox Hunt Lane PMB 176, Bear, DE 19701." As subsequently detailed in this affidavit, this address matches the return address of all drug packages received in subsequent undercover purchases from MDPRO.

Undercover Purchases of Controlled Substances from MDPRO

47. Between June 12, 2013 and September 3, 2013, using an undercover Silk Road user account that I created and controlled, I made four separate undercover purchases of controlled substances from MDPRO.

48. I placed the orders by utilizing the TOR browser to access The Silk Road website. Once on the Silk Road website, I activated links which lead me to MDPRO's vendor profile page. MDPRO's vendor page displayed various controlled substances for sale. The vendor page also displayed information that had been posted by MDPRO that would assist potential customers in placing a successful order with MDPRO for controlled substances. A screen capture of MDPRO's vendor profile page, captured on June 12, 2013, is attached to this affidavit as Exhibit 3.

49. All of the undercover purchases made from MDPRO were made utilizing Bitcoins that I previously acquired from a Bitcoin exchanger.

50. After placing an order with MDPRO, all of the packages I received were printed with a return address of "Samples Unlimited, 26 Fox Hunt Dr PMB 176, Bear, DE 19701" and contained a printed USPS tracking number.

June 12, 2013 undercover purchase of Oxycontin

51. On June 12, 2013, I located an advertisement placed by MDPRO for "Two tablets 80mg Oxycontin."¹⁹ MDPRO offered each lot of two Oxycontin 80mg tablets in exchange for 0.90 Bitcoins per lot. At the time of the transaction, 0.90 Bitcoins was worth approximately \$100.89. I added the two lots (a total of four 80 mg Oxycontin tablets) to my undercover "Shopping Cart" by activating the "Add to Cart" function. MDPRO charged an additional 0.09 Bitcoins for shipping. The total cost for four Oxycontin 80mg tablets, including shipping, was 1.88

¹⁹ Oxycontin is a brand name for Oxycodone.

Bitcoins. At the time of the transaction, the total cost was approximately \$211.35.

52. 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.

53. I entered an undercover name and an undercover commercial post office box as the shipping address.²⁰ 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.

54. On June 17, 2013, I received a USPS Priority mail package at the undercover commercial post office box that I supplied to MDPRO as the shipping address for the Oxycontin tablets. The package was addressed to the undercover name I supplied MDPRO. The package was printed with a return address of "Samples Unlimited, 26 Fox Hunt Drive, PMB 176, Bear, DE 19701" and had a USPS tracking number. The USPS tracking number showed the package originated in Newark, Delaware on June 13, 2013.

²⁰ The undercover commercial post office box referred to in this affidavit was located in Seminole County, Florida.

55. Contained in the package, I located a shipping invoice from "Samples Unlimited" showing an invoice for a "Sample Order" of "Sour Patch watermelon candy" and an additional envelope containing a bulky item. Inside the envelope, I located a sealed box of Sour Patch watermelon candy. Concealed inside the Sour Patch watermelon candy box was a silver, heat-sealed, Mylar anti-static type bag which contained a plastic baggie. The plastic baggie contained four Oxycontin 80mg tablets.

56. I accessed the Silk Road website and activated the "finalize" feature under the tab "orders." Activating this feature allowed the Bitcoins held in escrow to be transferred to MDPRO.

June 19, 2013 undercover purchase of Valium

57. On June 19, 2013, I located an advertisement placed by MDPRO for "Valium²¹ (Generic) 15mgx5." MDPRO was selling lots of five Diazepam 15mg tablets in exchange for 0.10 Bitcoins per lot. I added two lots (a total of 10 tablets) to my undercover "Shopping Cart" by activating the "Add to Cart" function. MDPRO charged an additional 0.09 Bitcoins for shipping. The total cost of 10 Diazepam 15mg tablets, including shipping, was 0.29 Bitcoins. At the time of the transaction, 0.29 Bitcoins was worth approximately \$31.02.

58. 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

²¹ Valium is name branding for Diazepam, which is a Schedule IV controlled substance.

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

59. 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.

60. On June 24, 2013, I received a USPS Priority mail package at the shipping address that I supplied to MDPRO for the Diazepam tablets. The package was addressed to the undercover name I supplied. The package was printed with a return address of "Samples Unlimited, 26 Fox Hunt Drive, PMB 176, Bear, DE 19701" and had a USPS tracking number. The USPS Tracking number showed that the package originated in Bear, Delaware on June 21, 2013.

61. Contained in the package, I located a shipping invoice from "Samples Unlimited" showing an invoice for a "Sample Order" of "Airheads" candy and an additional envelope that contained a bulky item. Inside the additional envelope, I located a sealed box of Airheads candy. Concealed inside the Airheads candy box, I located a silver, heat-sealed, Mylar anti-static type bag which contained a plastic baggie. The plastic baggie contained ten Diazepam 15mg tablets.

62. I accessed the Silk Road website and activated the “finalize” feature under the tab “orders.” Activating this feature allowed the Bitcoins that were held in escrow to be transferred to MDPRO.

63. This package appeared on **BOLLES'** USPS shipment history.

August 2, 2013 undercover purchase of Alprazolam and Adderall

64. On August 2, 2013, I located advertisements placed by MDPRO offering Alprazolam²² 2mg and Adderall²³ 20mg tablets for sale. MDPRO was selling lots of five Adderall 30mg tablets in exchange for 0.95 Bitcoins per lot. MDPRO advertised the Adderall as being manufactured by Qualitest Pharmaceuticals.²⁴ I added four lots (20 tablets) to my undercover “Shopping Cart” by activating the “add to cart” function. The cost for 20 Adderall 30mg tablets was 3.8068 Bitcoins, which, at the time of transaction, was approximately \$399.59.

65. MDPRO was also selling lots of five Xanax²⁵ 2mg tablets in exchange for 0.211 Bitcoins per lot. MDPRO listed the Xanax as “ONAX” brand.²⁶ I added two lots (10 tablets) to my undercover “Shopping Cart” by

²² Alprazolam is a Schedule IV controlled substance.

²³ Adderall is brand name Mixed Amphetamine Salts, a Schedule II controlled substance.

²⁴ Qualitest Pharmaceuticals is an American pharmaceutical company that produces generic drugs.

²⁵ Xanax is a brand name for Alprazolam, a Schedule IV controlled substance.

²⁶ ONAX Alprazolam is manufactured by Safe-Pharma, a pharmaceutical company operating in India.

activating the "add to cart" function. The cost of 10 Xanax 2mg tablets was 0.422 Bitcoins, which, at the time of transaction, was approximately \$43.24.

66. 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.

67. 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.

68. On August 9, 2013, I received a USPS Priority mail package at the undercover commercial post office box that I supplied to MDPRO as the shipping address for the Adderall and Xanax order. The package was addressed to the undercover name I supplied.

69. The package listed a return address of "Samples Unlimited, 26 Fox Hunt Drive, PMB 176, Bear, DE 19701" and had a USPS tracking number. The USPS tracking number showed that the package originated in Bear, Delaware on August 7, 2013.