UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. DAREN JAMES REID, Defendant.	**Filed Under Seal** Case No. 1:20-MJ-250

AFFIDAVIT IN SUPPORT OF
A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Jacob Ellis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Food and Drug Administration – Office of Criminal Investigations (FDA-OCI) since February 2015. I have received training related to cybercrime investigations, and am familiar with the tactics, methods and techniques of persons who unlawfully market and distribute drugs via internet websites. I have participated in the execution of numerous search warrants, of which the majority involved misbranded, adulterated, or stolen medical products and drugs. Before working for FDA-OCI, I conducted criminal investigations into violations of credit card fraud, identity theft, money laundering, and wire/mail fraud as a Special Agent with the United States Secret Service for approximately ten years. I have experience investigating violations of narcotics trafficking offenses and computer-facilitated crimes. I have participated in the execution of numerous search and arrest warrants pertaining to illegal narcotics, paraphernalia related to the use of illegal narcotics, monies or proceeds derived from the sale of illegal narcotics, and records, ledgers, and documents pertaining to the purchase and sale of controlled substances. I have also conducted and

participated in narcotics investigations resulting in the arrests and convictions of drug distributors, and seizures of controlled substances. As a result, I am familiar with the use, effects, distribution techniques, appearance, and method of manufacture of controlled substances. Additionally, I am familiar with the functioning and structure of narcotics markets operating on internet-based Darknets ("Darknet markets") including the operations of Darknet market administrators ("admins"), the sellers on such markets ("vendors"), and the purchasers on such markets ("buyers").

2. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. Rather, I make this affidavit in support of an application for a criminal complaint and arrest warrant for Daren James Reid ("REID"). I submit that this affidavit sets forth probable cause to believe that REID has distributed, and possessed with intent to distribute, a controlled substance, oxycodone, in violation of Title 21, United States Code, Section 841(a).

TECHNICAL BACKGROUND

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

be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

4. Bitcoin[1] is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

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

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

7. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity.

[1] As of August 5, 2020, the value of one Bitcoin was approximately $11,432.10 USD based on Morningstar for Currency and Coinbase for Cryptocurrency.

Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

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

9. Darknet sites, such as Empire, Cryptonia, and Apollon, primarily operate on the Tor network. The Tor network ("Tor") is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" or "onion services" ("hidden services") on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, which end in ".onion" and can only be accessed through specific web browser software designed or adapted to access the Tor network. These addresses are either 16 characters long (version 2 or v2) or 56 characters long (version 3 or v3).

PROBABLE CAUSE

12. Since in or about April 2019, FDA-OCI has been conducting a criminal investigation of a darknet market vendor operating under the name IMPERIALROYALTY. A darknet market is a hidden commercial website that operates via the darkweb. Darknet markets operate as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods, as well as the sale of legal products.

13. IMPERIALROYALTY was selling and distributing prescription opioid pills on a number of darknet marketplaces, to include Dream, Wall Street, and Apollon. Dream and Apollon Markets are no longer operating, and Wall Street Market was taken down by law enforcement. IMPERIALROYALTY continued to sell and distribute prescription opioid pills via encrypted email communications.

14. IMPERIALROYALTY amassed over 1,100 sales of prescription pills on Dream Market. After Dream Market closed in March 2019, IMPERIALROYALTY migrated to Wall Street Market and completed approximately 70 sales of prescription pills before that market's takedown in April 2019. Following the takedown of Wall Street Market, IMPERIALROYALTY had their own private vendor shop and only provided a limited number of customers with a link to the site. For unknown reasons, IMPERIALROYALTY returned to operating via a market and joined Apollon Market on or about November 22, 2019, until that market also went down in early 2020.

15. On each of the darknet markets, IMPERIALROYALTY advertised the sale of illegal narcotics. For example, on Wall Street Market, IMPERIALROYALTY listed for sale "ALG 265 Oxycodone 30MG Pharm Fresh Guaranteed." The listing further described that

"ALG/265 Oxycodone 30 MG manufactured by Alvogen, Inc. All Products are Pharmacy Fresh Guaranteed!! No Fake or Pressed Items."

UNDERCOVER PURCHASES

16. On or about April 8, 2019, an undercover Federal Bureau of Investigation ("FBI") agent ordered 10 oxycodone pills from IMPERIALROYALTY via Wall Street Market. The pills were shipped to Manassas, Virginia and originated from the Miami, Florida area. The return address of the package included a fictitious name and address. The pills were inside of a yellow padded manila envelope. Within the yellow padded manila envelope was a sealed black Mylar package. Within this package, there was a tightly wrapped ball of blue packing tape. Within the tape was aluminum foil. Inside of the aluminum foil, was a white piece of paper containing ten blue pills. Based on my training and experience, this packaging process was an attempt by the sender to conceal the contents of the package. On or about April 11, 2020, the FBI received 10 pills as ordered from IMPERIALROYALTY. The pills were stamped "M" on one side and "30" on the other. The pills were sent to the Drug Enforcement Administration ("DEA") laboratory for testing and tested positive for oxycodone.

17. In February 2020, an undercover FDA-OCI agent ordered 22 Oxycodone pills from IMPERIALROYALTY via encrypted email address imperialroyalty@secmail.pro (hereinafter, "IMPERIALROYALTY Encrypted Email Address"). This email address was previously listed on dark web markets as a way to contact IMPERIALROYALTY. On or about February 5, 2020, IMPERIALROYALTY provided a bitcoin address ending Umgt as a payment address (hereinafter, "IMPERIALROYALTY First Direct Deal Address") to the undercover FDA-OCI agent. On or about February 5, 2020, the undercover FDA-OCI agent sent bitcoin to the IMPERIALROYALTY First Direct Deal Address to purchase controlled substances. On or

about February 10, 2020, the FDA-OCI agent received 22 pills as ordered from IMPERIALROYALTY. These pills were white in color, bearing the letters "RP" on one side and "30" on the other. Based on my training and experience, these markings are consistent with the FDA approved Oxycodone Hydrochloride 30mg tablets produced by Rhodes Pharmaceuticals. The pills were sent to the FDA lab for testing and tested positive for oxycodone.

18. The pills were shipped to Alexandria, Virginia, in a U.S. Postal Service ("USPS") Priority Mail Express envelope from the Miami, FL area. The return address of the package included a fictitious name and address. The pills in this package were wrapped in a napkin and then secured with black duct tape with multi-colored stripes, then packaged in a black Mylar style zip lock bag, followed by a yellow padded envelope before finally being placed in the USPS Priority Mail envelope. Based on my training and experience, this was done in an effort to deter law enforcement efforts from determining the contents of the package. Below is a photo of this packaging.

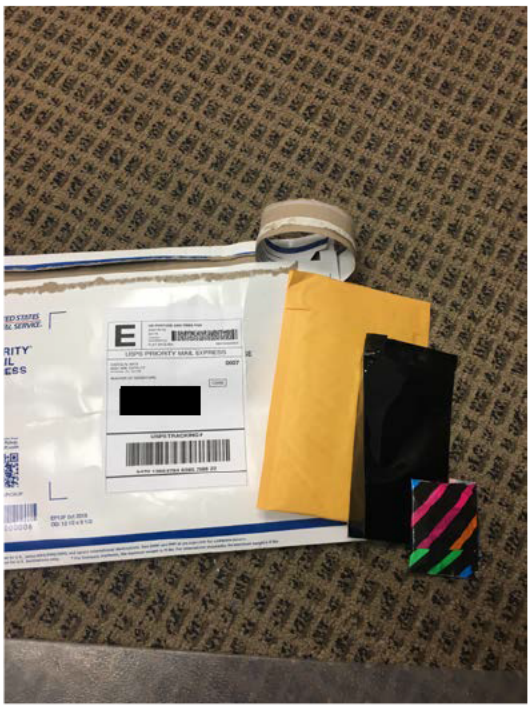
19. In March 2020, an undercover FDA-OCI agent ordered 25 Oxycodone pills from IMPERIALROYALTY via the IMPERIALROYALTY Encrypted Email Address. On or about March 13, 2020, IMPERIALROYALTY provided a bitcoin address ending G3RW as a payment address (hereinafter, "IMPERIALROYALTY Second Direct Deal Address") to the undercover FDA-OCI agent. On or about March 13, 2020, the undercover FDA-OCI agent sent bitcoin to the IMPERIALROYALTY Second Direct Deal Address to purchase controlled substances. On or about March 19, 2020, the FDA-OCI agent received 25 pills as ordered from IMPERIALROYALTY. These pills were white in color, bore the letters "RP" on one side and "30" on the other, the same as the February purchase. The pills were sent to the FDA lab and tested positive for oxycodone.

20. The pills were shipped to Alexandria, Virginia, in a USPS Priority Mail Express envelope from the Miami, FL area. The return address of the package included a fictitious name and address. The pills in this package were wrapped in a napkin and then secured with purple duct tape, then packaged in a black Mylar style zip lock bag, followed by a yellow padded envelope before finally being placed in the USPS Priority Mail envelope. This packaging was consistent with the purchase in February 2020. Below is a photo of this packaging.

21. In May 2020, an undercover FDA-OCI agent ordered 25 Oxycodone pills from IMPERIALROYALTY via the IMPERIALROYALTY Encrypted Email Address. On or about May 1, 2020, IMPERIALROYALTY, via the IMPERIALROYALTY Encrypted Email Address, provided a bitcoin address ending opCN as a payment address (hereinafter, "IMPERIALROYALTY Third Direct Deal Address") to the undercover FDA-OCI agent, and also provided a list of drugs the vendor had in stock. This list included Oxycontin in 20mg, 30mg, 60mg and 80mg, Hydromorphone Hydrochloride 8mg in three different forms, and Oxycodone 10mg. IMPERIALROYALTY ended the email by stating, in sum and substance, that if the undercover FDA-OCI agent was not interested in anything on the list then they would advise when they had more Oxycodone 30mg pills like the previous purchases. On or about May 1, 2020, the undercover FDA-OCI agent sent bitcoin to the IMPERIALROYALTY Third Direct Deal Address to purchase controlled substances. On or about May 5, 2020, the FDA-OCI agent received 25 of Oxycodone 30mg pills, as ordered from IMPERIALROYALTY. The pills received were brown in color, bearing the letters "RP" on one side and "30" on the other. Based

on my training and experience, the appearance and markings on the pills are consistent with the FDA approved Oxycontin 30mg pills produced by Purdue Pharma ("Oxycontin" is a brand name of oxycodone). The pills were sent to the FDA lab and tested positive for oxycodone.

22. The pills were shipped to Alexandria, Virginia, in a USPS Priority Mail Express envelope. The purchase made on or about May 1, 2020 was shipped from the Miami, FL area. The return address of the package included a fictitious name and address. The pills in this package were wrapped in a napkin and then secured with black duct tape with multi-colored stripes, then packaged in a black Mylar style zip lock bag, followed by a yellow padded envelope before finally being placed in the USPS Priority Mail envelope. This packaging was consistent with the purchases in February and March. Below is a photo of the packaging.



ONLINE AND IP ADDRESS CONNECTION

23. An analysis of the ImperialRoyalty First Direct Deal Address revealed transfers

from this Bitcoin address to a Bitcoin address associated with a Paxful[2] account in the name "yingyang1883" and created with email address ying.yang1883@gmail.com. Records received from Paxful for the account "yingyang1883" show that the account was accessed via Internet Protocol (IP) addresses 174.253.160.54 on 01/20/2020, and 66.135.138.195 on 01/22/2020. These IP addresses resolve to Verizon and Access Media Holdings, respectively. These Paxful records further show the account "yingyang1883" was accessed via IP address 2601:583:300:c8f0:844c:f664:c1a5:92a2 on 11/23/2019. This IP address resolves to Comcast. Records obtained from Verizon for IP address 174.253.160.54 showed that phone number [redacted] 0319 was assigned IP address 174.253.160.54 on 1/20/2020. The records for the [redacted] 0319 phone number did not list a subscriber or an address associated with the account. Based on my training and experience, drug traffickers often use "drop phones," and do not list a name or an address on the subscriber records to evade law enforcement. A drop phone is typically established on a month to month basis without the need for a credit check or long-term contact.

24. Records obtained from Comcast related to IP addresses 2601:583:300:c8f0:844c:f664:c1a5:92a2, which was used to log into the aforementioned Paxful account on or about November 23, 2019 revealed the subscriber to be Daren Reid, with a service address of [redacted] Hallandale Beach FL, 33009, and a billing address of [redacted], Fort Lauderdale, FL 33301 (hereinafter, "REID'S RESIDENCE") and telephone number [redacted] 0319. The service was disconnected in December 2019.

25. Records obtained from Access Media Holdings for IP address 66.135.138.195

[2] Paxful.com is a website trading platform which allows individuals to advertise the sale of virtual currency for fiat currency.

revealed that the account is registered to [redacted] at [redacted], Fort Lauderdale, Florida. Access Media Holdings could not locate a specific subscriber for this account. However, law enforcement believes that this account is associated with Daren Reid. IP address 66.135.138.195 was used to access accounts for darenreid85@gmail.com, ying.yang1883@gmail.com, and Paxful "yingyang1883."

26. Records obtained from Google show that account ying.yang1883@gmail.com was accessed via IP address 66.135.138.195 on 02/26/2020 and 02/27/2020. This is the same IP address as was used to access Paxful account "yingyang1883" on 01/22/2020, as described in Paragraph 23. Ying.yang1883@gmail.com was established on 06/09/2017.

27. Based on public internet database searches, it was also determined that Daren REID is associated with email address darenreid85@gmail.com. Records obtained from Google show that the email address darenreid85@gmail.com was accessed by IP address 174.253.160.54 on 01/20/2020. This is the same IP address as was used to access Paxful account "yingyang1883" on 01/20/2020, as described in Paragraph 23 above. Further, these records show that the email address darenreid85@gmail.com was accessed via IP address 66.135.138.195 35 times between 11/28/2019 and 03/19/2020. This is the same IP address as was used to access Paxful account "yingyang1883" on 01/22/2020, as described in Paragraph 23 above. The Google records further show that darenreid85@gmail.com was established on 11/01/2011 and show a recovery phone number of [redacted]0319, the same phone number referenced in Paragraph 24 which was found in the internet subscriber account used to access the "yingyang1883" Paxful account.

28. In May 2020, law enforcement obtained a search warrant for email accounts ying.yang1883@gmail.com and darenreid85@gmail.com. A review of results revealed an image

in the darenreid85@gmail.com email account showing a large collection of pills stamped "M" on one side and "30" on the other side (the same stamps as on pills purchased by the FDA-OCI undercover agent on or about April 8, 2020, as further described in Paragraph 16) and a printed image of the word "OxyFlight." Based on my training and experience, pills shown in this image are visually consistent with FDA approved genuine 30 mg Oxycodone Hydrochloride pills manufactured by Mallinckrodt Pharmaceuticals. A copy of the image found is below for reference.

29. Additionally, law enforcement found a photographic image in the darenreid85@gmail.com email account which showed a computer screen displaying a Dwolla financial transfer. Dwolla is an e-commerce company that provides an online and mobile payment system for the transfer of funds. This image displayed a contact email address of darenreid85@gmail.com and a bitcoin address of 1PrswF8ENq55EvMZJTrh8BCBSuZ8q (hereinafter, "REID REFUND ADDRESS").

30. In May 2020, law enforcement conducted virtual currency analysis to examine the REID REFUND ADDRESS. This analysis showed this wallet received a total of $37,869.01 between August 2012 and November 2012 of which $37,212.90 came directly from the dark web

market Silk Road Marketplace. Silk Road Marketplace was seized by the FBI in October 2013.

31. Through further analysis of the REID REFUND ADDRESS and the name "OxyFlight," law enforcement searched the seized Silk Road Marketplace servers which revealed a vender by the name "OxyFlight" operating on Silk Road Marketplace selling Oxycodone. OxyFlight had approximately 2,500 sales totaling approximately $540,000. Further, several bitcoin wallets associated as payment withdrawal addresses for funds from Silk Road Marketplace to OxyFlight make reference to the email address darenreid85@gmail.com.

32. Additionally, on June 2, 2020, law enforcement obtained authorization for a pen register/trap and trace ("PRTT") device for aforementioned Access Media Holdings' account. A review of data collected from the PRTT revealed approximately 10 connections between IP address 66.135.138.195 and TOR relays from on or about July 2, 2020 to on or about July 28, 2020, with four of those connections occurring on July 28, 2020. Based on my training and experience, connections with TOR relays indicate a user's intent to conceal its user's identities and their online activity from surveillance and traffic analysis by separating identification and routing. Such activity typically occurs when a user is accessing or attempting to access the dark web – where the Darknet Markets described here are accessed.

33. On July 20, 2020, law enforcement served a 2703(d) order to Instagram, owned by Facebook Inc., for records pertaining to accounts ying.yang1883, purplelitmedia, and nevermissbrunch. Purplelitmedia and nevermissbrunch are social media profiles that law enforcement observed while conducting searches related to Daren REID via public internet searches.

34. Documents returned from Instagram for the ying.yang1883 account show it was created on October 16, 2019 with a registered email address of ying.yang1883@gmail.com.

Further, these documents show the ying.yang1883 Instagram account was accessed 125 times between January 4, 2020 and July 20, 2020 by IP address 66.135.138.195, the same IP address which was used to access the yingyang1883 Paxful account and the darenreid85@gmail.com email account.

35. Documents returned from Instagram for the purplelitmedia account show it was created on May 23, 2018 with a registered email address of purplelitmusic@gmail.com and a verified phone number of [redacted]0319, the same phone number referenced above. Further, this Instagram account was accessed by IP address 66.135.138.195 as recently as July 17, 2020.

36. Documents returned from Instagram for the nevermissbrunch account show that it was created on January 28, 2019 with the first name Daren and with an email address of nevermissbrunch@gmail.com. Further, this Instagram account was accessed by IP address 66.135.138.195 as recently as July 12, 2020.

37. On August 6, 2020, law enforcement visited the [redacted] apartment building located at [redacted], Fort Lauderdale FL 33301 and identified themselves to the building maintenance manager (hereinafter, "Manager"). The Manager informed law enforcement that Daren Reid lives in apartment [redacted], and further provided a contact number for REID as [redacted]0319.

Surveillance

38. On May 28, 2020, law enforcement conducted surveillance of REID while REID was driving a 2007 green Jeep bearing Florida license plate number APPL51 (hereinafter, "REID'S VEHICLE"). REID was identified by law enforcement based on the photograph on his Florida driver's license that was obtained through the Florida Department of Motor Vehicle database. On this date, REID'S VEHICLE was observed at [redacted], Fort Lauderdale,

Florida 33301 (the building of REID'S RESIDENCE). Research of the vehicle registration information revealed that REID'S VEHICLE was registered to REID at [redacted], Hallandale Beach FL 33009, his former address.

39. On May 29, 2020, law enforcement observed REID exit the building of REID'S RESIDENCE, enter the driver's side of REID'S VEHICLE, and depart the area. Law enforcement observed REID'S VEHICLE arrive at the U.S. Post Office located at 3225 N. Hiatus Road, Fort Lauderdale, FL 33345 (hereinafter, "USPS"). Law enforcement then observed REID place an unknown number of white envelopes in the drive through blue USPS mailbox. The below photos show REID in REID'S VEHICLE placing the envelopes in the blue USPS mailbox.

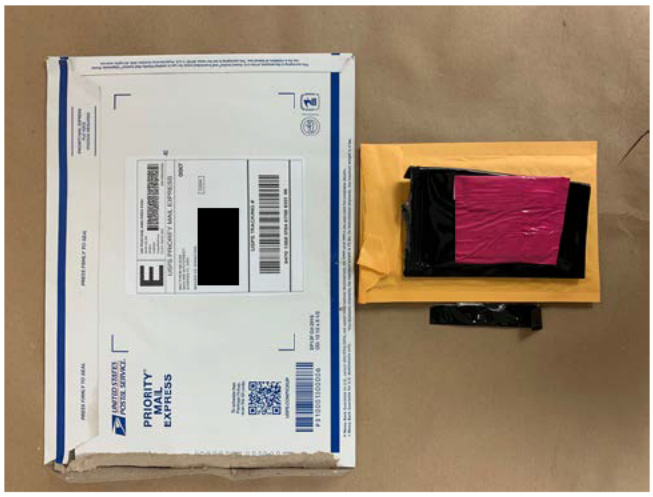
40. Law enforcement observed REID depart USPS in REID'S VEHICLE and arrive at a shopping mall. REID was observed entering the shopping mall with a black backpack with "Diamond" inscribed on it, and a white plastic bag. Law enforcement observed REID depart the shopping mall in REID'S VEHICLE and return to the building of REID'S RESIDENCE.

41. Shortly thereafter, an Inspector with the U.S. Postal Inspection Service ("USPIS") retrieved two Priority Mail envelopes from the blue USPS mailbox, which were similar to the packages REID placed inside the mailbox. Those packages were seized by USPIS for further investigation. The Priority Mail envelopes were addressed to individuals located in Naperville, Illinois and Tigard, Oregon. The packages were similar to packages previously received from IMPRIALROYALTY by the undercover FDA-OCI agent due to the common method of postage, type of shipping used, and package size and weight. Further, both parcels bore a label from a company that only accepts cryptocurrency as payment for postage purchased, and both came from account C26321 with the postage company. Previous parcels purchased from IMPERIALROYALTY by undercover law enforcement bore postage from the same account. Both parcels bore a return name and address of Matthew Nelson, 9633 NW 45th Street Sunrise, FL 33351.

42. Law enforcement subsequently contacted the intended recipient on the package that had been seized from the blue mailbox destined for Naperville, Illinois. The package was

hand-delivered to Illinois by law enforcement. On or about June 5, 2020, Witness #1 was interviewed by law enforcement in Naperville, Illinois. Witness #1 refused to provide information to law enforcement and denied ordering a package. The second package, which was destined for Oregon, was returned back to circulation and was allowed to be delivered as per normal USPS procedures as to not alert REID that numerous packages had been intercepted.

43. On or about June 12, 2020, law enforcement obtained a search warrant issued in the Northern District of Illinois for the parcel destined for Naperville, Illinois. Upon inspection, this parcel contained 30 light blue pills marked with "224," which, based on my training and experience, are visually consistent with Oxycodone Hydrochloride 30mg pills manufactured by Sun Pharmaceutical Industries. Further, several layers of packaging were used to hide the contents of the package. Specifically, the pills were wrapped and taped with purple tape, then placed in a black Mylar zip lock bag, then a padded brown envelope, and then in the USPS priority mail parcel. This style of packaging is consistent with the packing received through all undercover purchases with IMPERIALROYALTY between February 2020 and May 2020. The pills were sent to the FDA lab for testing and tested positive for oxycodone. The below photo shows the packaging described herein and mailed by REID on May 29, 2020.



CONCLUSION

44. Based on the above undercover purchases, online investigation, and surveillance, I submit there is probable cause to believe that Daren James REID violated Title 21 U.S.C. § 841(a)(1) (distribution, and possession with intent to distribute, controlled substances).

Respectfully submitted,

Jacob M Ellis

Jacob Ellis
Special Agent
FDA – Office of Criminal Investigations

Subscribed and sworn to in accordance with Fed. R. Crim. Proc. 4.1 by telephone on September 3, 2020.

IDD

The Honorable Ivan D. Davis
United States Magistrate Judge
Eastern District of Virginia