AFFIDAVIT

I, PAUL COX, being duly sworn, declare and state as follows:

1.   I am a Special Agent for the Food and Drug Administration-Office of Criminal Investigations ("FDA-OCI"). I am currently assigned to the Kansas City Field Office as a member of the Cybercrimes Investigation Unit. My current duties include investigating violations of the Federal Food Drug and Cosmetic Act and other violations of the United States Criminal Code. I have been employed as a Special Agent since November 2012. Through the course of my duties, I have conducted numerous investigations into the distribution of counterfeit, misbranded, and adulterated drugs and controlled substances via the darknet[1] and United States Postal Service, and personally executed more than seventy-five undercover purchases of drugs via the darknet in exchange for cryptocurrency.

2.   For the reasons set forth below, there is probable cause to believe that **KEVIN OMBISI** and **ERIC RUSSELL, JR.** did knowingly and willfully conspire with each other and others to distribute a mixture and substance containing a detectable amount of methamphetamine, a Schedule II controlled substance, in violation of Title 21, United States Code, Section 846 (Conspiracy); and that **KEVIN OMBISI** did knowingly and willfully distribute a mixture and substance containing a detectable amount of methamphetamine, a Schedule II controlled substance, in violation of 21, United States Code, Section 841 (Unlawful Distribution of Controlled Substances).

---

[1] The darknet is a portion of the internet that is not indexed by search engines and requires special software that encrypts and anonymizes internet traffic for both those browsing and hosting websites on the darknet. Because these protocols limit the ability of governments and law enforcement to track the usage and hosting of the sites, the darknet includes a large quantity of websites that exist primarily as marketplaces for illicit substances and services.

3.   The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel (collectively referred to as "Agents") and witnesses. This affidavit is intended to show merely that there is sufficient probable cause to support a criminal complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

4.   The FDA-OCI, and other law enforcement agencies, are investigating the illegal distribution of counterfeit Adderall[2] by a vender selling controlled substances on the darknet and through encrypted messaging (referred to in this affidavit as "VENDOR-1"). Through the course of this investigation, Agents made a number of undercover purchases from VENDOR-1 that were mailed from Texas to addresses in the Western District of Tennessee as well as to areas in Kansas and Missouri.

5.   In November 2019 VENDOR-1 advertised "100% AUTHENTIC Adderall Brand 30mg USA to USA SUPER FAST SHIPPING *FREE EXTRA PILLS PROMO*" on the darknet marketplace Empire Market.[3] VENDOR'1-s Empire Market sales page noted "Over 2000 5 Star Reviews," and indicated "3657 sold since April 24, 2019." On three occasions, in November 2019, February 2020, and June 2020, agents from DEA made undercover purchases of purported

---

[2] Adderall is a brand name, Schedule II amphetamine used to treat attention-deficit hyperactivity disorder, among other uses. *See* www.dea.gov/factsheet (last visited Feb. 4, 2021).

[3] Empire Market was a marketplace where one could find a variety of illicit drugs and services available for purchase from vendors throughout the world, but it ceased operations after August 2020. From my training and experience, I know that darknet marketplaces, and the Empire Market in particular, resemble other legitimate e-commerce websites like Amazon or eBay in many respects. For example, customers who purchase items from vendors on the Empire Market can leave reviews for their transactions. These reviews and the good or bad reputation associated with them are one of the few metrics that allow potential customers of illicit goods or services to anticipate the likelihood that the anonymous seller will complete the transaction.

Adderall from VENDOR-1 on Empire Market in exchange for bitcoin (hereafter "BTC") cryptocurrency.[4] In each instance, a package was delivered to the undercover address provided at the time of purchase, located in the Western District of Tennessee, and the contents of these purchases appeared consistent with what was advertised for sale on the Empire Market: amphetamine-based prescription drug tablets, orange in color, bearing pill markings consistent with prescription amphetamine-based drugs, specifically Adderall (collectively referred to as "Three Drug Parcels"). However, subsequent DEA laboratory testing revealed that the drugs received in the Three Drug Parcels did not contain amphetamine, the active pharmaceutical ingredient contained in Adderall, but in fact contained methamphetamine, a Schedule II controlled substance.

6.   The postage on the Three Drug Parcels was identified as pre-printed postage purchased through a United States Postage Reseller,[5] hereafter "Postage Reseller-1." Analysis of the information associated with the Postage Reseller-1 account used to ship the Three Drug Parcels, including shipping activity and payment records, led Agents to identify **OMBISI** as the true account holder of the Postage Reseller-1 account. In addition, surveillance, GPS location data, and closed-circuit television place **OMBISI** at various post offices depositing packages using the Postage Reseller-1 account.

---

[4] Bitcoin (BTC) is a type of cryptocurrency. Cryptocurrency is a virtual currency used as a substitute for fiat currency (i.e. government-issued money, such as the U.S. dollar) to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Individuals can acquire BTC through exchanges, BTC ATMs, or directly from other people. BTC allows users to transfer funds more anonymously than is possible through traditional banking and financial systems. Although cryptocurrencies, such as BTC, have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, such as money laundering, and to purchase illegal goods and services.

[5] Through a Postage Reseller, individuals can purchase and print official United States Postal Service stamps and shipping labels using an account that is often associated with a monthly subscription.

7.   In addition to the three purchases made through Empire Market, Agents made ten (10) undercover purchases of purported Adderall from VENDOR-1 through Wickr,[6] an encrypted messaging application, in exchange for BTC cryptocurrency. Specifically, on December 10, 2020, Agents placed an order through Wickr for Adderall and provided an undercover address in the Western District of Tennessee. That same day, Agents observed **OMBISI** at the Almeda post office in Houston, Texas, carrying a weighted bag. Shortly thereafter, Agents intercepted a package at the same Texas post office that was destined for the undercover address in the Western District of Tennessee. Thereafter, on January 27, 2021, after Agents placed another order through Wickr, providing an undercover address in Kansas, **OMBISI** was observed mailing packages at the Almeda post office in Houston, Texas; a package addressed to the undercover address was later retrieved from the same post office.

8.   During the course of this investigation, Agents conducted blockchain[7] analysis on seven (7) of the undercover Wickr purchases between January 22, 2020 and June 17, 2020. In the course of these purchases, Agents transferred a total of approximately 0.30461216 BTC cryptocurrency to seven (7) unique BTC wallet[8] addresses provided by VENDOR-1 for the purposes of completing the purchase. Based on the analysis:

   a.   four (4) of these undercover purchases are a part of a cluster of

---

[6] VENDOR-1 provided Agents with its Wickr username following the November 2019 Empire Market transaction. Wickr is an encrypted communication application that allows individuals to communicate via text and voice, and can be used on a cellular telephone. Wickr is used by individuals involved in the trafficking of counterfeit drugs because of the ability for senders of messages to set a self-destruct time for messages, as well as security features which notify senders of messages when parties to the conversation take a screenshot of messages.

[7] Blockchain is a publicly available ledger of cryptocurrency activity. Agents employ software to aid in tracing, clustering, and modeling data on the blockchain to obtain information regarding cryptocurrency transactions.

[8] A BTC wallet stores private and public keys used in BTC transactions. Private keys are used to make public keys, which can be converted to a BTC address. A BTC address is akin to a bank account number or email address that can be shown to receive payment. The owner of a private key has access to the funds stored on the corresponding BTC address. One person can have multiple BTC wallets and each wallet can store any number of private keys.

4

approximately one thousand one hundred and forty-nine (1,149) BTC wallet addresses, CM Wallet-1 hereafter; and

      b.   three (3) of the undercover purchases are a part of a cluster of approximately one thousand four hundred and eighty (1,480) BTC wallet addresses, CM Wallet-2 hereafter.

     9.   Agents conducted further blockchain analysis of the above-referenced seven transactions and examined business records associated with a peer-to-peer cryptocurrency exchanging service located in the European Union, P2P Exchanger-1 hereafter. They found the following:

      a.   An account registered in the name of "**KEVIN OMBISI**" received 10.36513383 BTC from CM Wallet-1, between October 04, 2019 and October 12, 2019; and

      b.   A second account registered to "**KEVIN OLANDO OMBISI**" received approximately 113.54868227 BTC, through approximately one hundred and seventy-four (174) transactions, between October 16, 2019 and April 20, 2020, from CM Wallet-1, and approximately 75.86273833 BTC, through approximately one hundred and five (105) transactions, between March 12, 2020 and June 01, 2020, from CM Wallet-2.

     10.   On approximately three (3) distinct occasions on December 4, 2019, and approximately two (2) distinct occasions on April 2, 2020, P2P Exchanger-1 business records indicate that the account registered to "**KEVIN OLANDO OMBISI**" was accessed by a computer assigned an IP address tied to **RUSSELL**. Specifically, the same IP address accessed an iCloud Account registered to "**Eric Russell**" on approximately nine thousand six hundred and forty-four (9,644) distinct occasions between August 02, 2019 and December 18, 2020, and internet company Comcast Communications business records indicate the IP address serviced **RUSSELL'S** residence as early as November 24, 2019 and at least as recently as May 12, 2020.   P2P

Explore Litigation Insights

DOCKET ALARM

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.