UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

No. 17-MJ-02370-GARBER

UNITED STATES OF AMERICA

v.

KEVIN C. FUSCO,
a/k/a, "POLIRA,"

Defendant.
_____/

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to October 14, 2003? _____ Yes __X__ No

2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to September 1, 2007? _____ Yes __X__ No

Respectfully submitted,

WIFREDO A. FERRER
UNITED STATES ATTORNEY

BY: _____

FRANCISCO R. MADERAL
ASSISTANT UNITED STATES ATTORNEY
Fla. Bar. No. 41481
99 N. E. 4th Street
Miami, Florida 33132-2111
TEL (305) 961-9159
FAX (305) 530-7976
francisco.maderal@usdoj.gov

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America)
v.)
KEVIN C. FUSCO, a/k/a, "POLIRA,") Case No. 17-MJ-02370-BARBER
)
)
)
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 9/2015-4/2016 in the county of Miami-Dade in the Southern District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
Title 21, United States Code, Sections 846 & 841(b)(1)(c)	Conspiracy to Distribute Controlled Substances
Title 18, United States Code, Sectiona 1956(h) & 1956(a)(1)	Conspiracy to Committ Money Laundering

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

Complainant's signature

Maria Isabel Vasallo, S/A, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: 3-9-17

Judge's signature

City and state: Miami, Florida

Barry L. Garber, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, MARIA ISABEL VASALLO, Special Agent with the Drug Enforcement Administration, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. That is, I am an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1), and in Title 21, United States Code, Section 878.

2. This affidavit is made in support of a criminal complaint charging Kevin FUSCO, a/k/a "POLIRA," with conspiracy to distribute narcotics, in violation of Title 21, United States Code, Section 846, and conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

3. I have not necessarily included in the affidavit each and every fact known to me about the matters set forth herein, but only those facts and circumstances that I believe are sufficient to establish probable cause for the Court to sign a criminal complaint.

4. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers and on my experience and training as a federal agent and the experience and training of other federal agents.

PROBABLE CAUSE

5. This application stems from an ongoing criminal investigation into drug dealers operating on criminal online marketplace websites, including a website known as the Nucleus Market.

6. In the course of this investigation, I have learned that the Nucleus Market website was one of many criminal marketplaces operating on The Onion Router ("Tor") network, otherwise known as the "dark web." From its inception in November 2014 to the date that it went offline in April, 2016, The Nucleus Market was designed to promote the anonymous sale of illegal items, such as narcotics, in exchange for Bitcoin and other, peer-to-peer crypto-currencies (also known as, virtual currencies).

7. As set forth in more detail below, probably cause exists that FUSCO was trafficking in narcotics and laundering in the proceeds of his activities using Bitcoin and the dark web, in conspiracy with the unknown administrator(s) of the Nucleus Market.

I. THE TOR NETWORK AND THE "DARK WEB"

8. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by their unique IP address. This number is used to route information between devices. Generally, when one device contacts a second device, the first device must be directed to the IP address of the second device. Moreover, when the first device contacts the second device, the first device provides its own IP address to the second device, so that the second device knows where to direct its response. Accordingly, the two connected devices (for instance, a home computer and the www.google.com website server) know each other's IP address.

9. The typical user may not know the IP address of a websites he visits. Typically, a user will type the domain name of the website—which commonly corresponds to a plain-language name for the website, *e.g.,* www.google.com—into the Uniform Resource Locator ("URL") bar at the top of their web browsers. This domain name will be transmitted to a Domain

Name System ("DNS") server, which then translates the domain name into the appropriate numerical IP address, and thereby allows the user to connect with the requested website.

10. However, if a user knows of a unique IP address for a particular website, generally[1] the user can type that IP address directly into the URL bar and access the website in that manner.

11. In addition, publicly available databases can be easily searched to obtain the IP address for any known URL and the registered owner and location of any IP address. Thus, with additional inquiry, most any URL or IP address can be traced to its owner and physical location.[2] This is problematic for anyone conducting criminal activity on the internet and wishing to remain anonymous.

A. User Anonymity Provided by the Tor Network

12. The Onion Router (Tor) network is a special network of computers distributed around the world designed to conceal the true IP addresses of the users of the network. Every communication sent through Tor is directed through numerous relays within the network—and

---

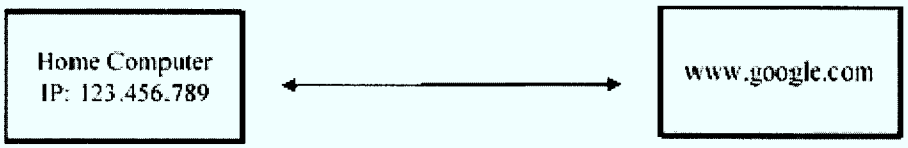
[1] The server or virtual server with a particular IP address can host multiple websites, in which case entering that particular IP address would not direct a user to a single website. However, if an IP address is associated with a single website, entering the IP address as described above would direct the user to that particular website.

[2] Private individuals operating home computers usually do not own and register their own IP address; instead, they subscribe to broadband accounts with ISPs, such as Comcast or AT&T, which in turn assign or lease an IP address to them (the subscriber). Nevertheless, the IP address can usually be traced to its assigned user at a given point in time using the ISPs records of which subscriber was assigned which IP address and when.

wrapped in a layer of encryption at each relay—such that the end recipient of the communication has no way of tracing the communication back to its true originating IP address.

13. In order to access the Tor network, anyone can simply download the Tor browser software and use it to access the internet. The user simply inputs a website IP address or URL into the Tor browser and the Tor browser automatically encrypts and routes the communication through several relays and then out to the destination so that the destination website can only see the IP address of the last (or "exit") relay and not the IP address of the device actually connecting to the destination website.

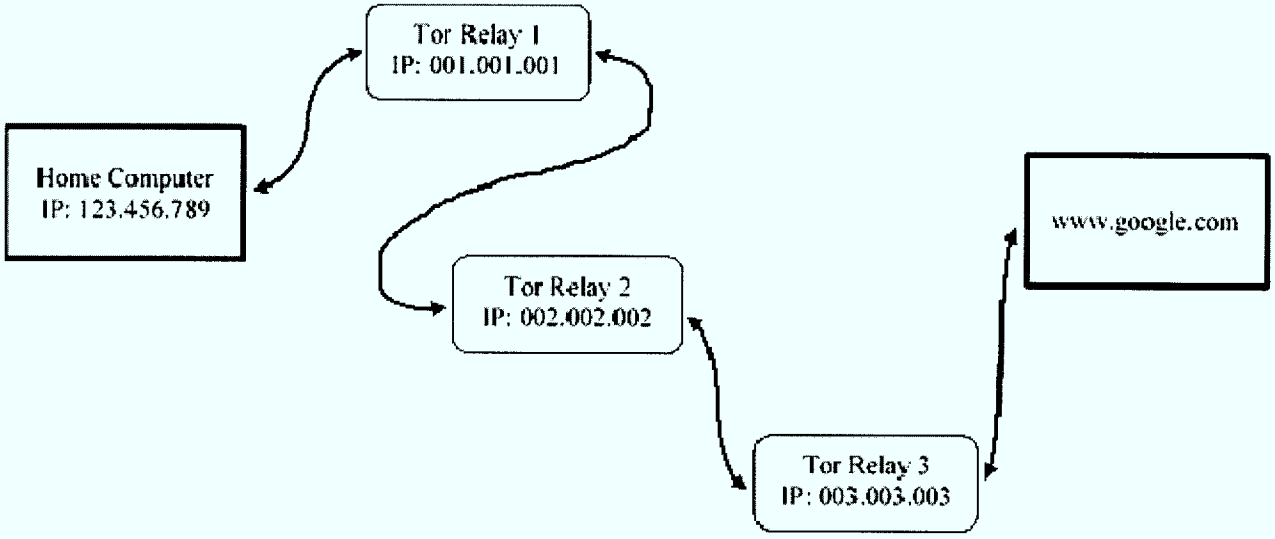
14. By way of illustration, in a standard internet communication, when a person connects to a website, that website can see that persons IP address:



In this illustration of a standard internet connection, the website www.google.com can see the home computer IP address (123.456.789) and, of course, the user of the home computer knew the URL, and therefore the IP address, of www.google.com, which the user had to type into his browser to connect to the website in the first place. Thus, each users' IP address is known to the other, and the owner and location of both can later be traced.

15. Similarly, any person monitoring the internet traffic at a point between the two would see the connection between IP 123.456.786 and www.google.com and know that those two devices were communicating.

16. On the other hand, in the case of a Tor network communication, when a person connects to a website, the traffic is encrypted and routed through multiple relays, and that website cannot see that persons IP address:



In this illustration of a Tor network connection, the website www.google.com cannot see the home computer IP address (123.456.789); instead it only sees the IP address of the device it is directly connected to, the third (or "exit") Tor relay, with IP address 003.003.003, which IP address cannot be traced back to the home computer user.

17. In addition, any person monitoring the internet traffic at a point between the home computer and www.google.com and would not know that those two devices were communicating. Instead, depending on the monitoring point, that person would only see the direct connections between the home computer and first (or "entry") Tor relay, between the first and second, or second and third Tor relays, or between the third (or "exit") Tor relay and www.google.com.

18. As with a standard internet connection, the user must have known the URL or IP address of the website in order to have directed a connection to it through the Tor network. Accordingly, although the IP address of the user is hidden from the website, the IP address of the website must be known to the user—the anonymity is only one-way.

19. The Tor network addresses this problem through a feature known as "hidden services."

B. Hidden Services: Website Anonymity Provided by the Tor Network

20. To achieve true, two-way anonymity, the Tor network also enables websites to operate inside the network in a manner that conceals the true IP address of the computer server hosting the website. Such "hidden services" operating on Tor have complex web addresses, generated in a computer algorithm, ending in ".onion." Unlike a standard URL, there is no way to retrieve a website server's true IP address from its .onion Tor address alone.

21. This alleviates the need for a Tor network user to know the true IP address of a website. Rather the user can direct his Tor browser to the .onion address, reach the website, and neither the user nor the website knows the other's IP address—two-way anonymity is achieved. This network of anonymous users and websites is the "Dark Web."

22. Criminals have taken advantage of the Dark web to create websites with online marketplaces dedicated to the trafficking of controlled substances and other illicit goods. Websites such as www.deepdotweb.com maintain an overview of illegal marketplaces operating on the Dark Web, and how-to guides such as: "How to Buy Drugs Online from Darknet Markets."[3]

---

[3] https://www.deepdotweb.com/2015/12/30/buy-drugs-online-from-darknetmarkets/

C. Description of the Nucleus Market

23. Nucleus provided an infrastructure that allowed buyers and sellers to conduct transactions online, in a manner similar to well-known online marketplaces such as eBay. Like eBay:

a. Nucleus functioned as an intermediary between buyers and sellers. Sellers created accounts on Nucleus to advertise their products, such as narcotics or hacked computer passwords, and buyers created accounts to browse sellers' products and purchase them; in this regard, Nucleus's website interface is similar to well-known online marketplaces;

b. Nucleus performed moderator and maintenance services, such as receiving complaints, providing technical assistance, and allowing customers to post reviews of Nucleus vendors. Nucleus also provided a means by which its users can communicate with its administrators and operators; and

c. Nucleus charged a commission from every transaction as a percentage of the sale price.

24. However, unlike legitimate online marketplaces, Nucleus was dedicated and designed to facilitate the sale of illegal narcotics, drug paraphernalia, firearms, and counterfeit and fraud-related goods and services. For example:

a. Illegal drugs, such as methamphetamines, heroin, and cocaine, were openly advertised and sold and were immediately and prominently visible on the Nucleus website. Some of the item categories listed on the Nucleus website were: "Fraud," "Drugs & Chemicals," "Counterfeit Items," "Weapons," and "Software & Malware";

b. The Nucleus website was specifically designed to facilitate illegal commerce by working to ensure the anonymity of its administrators, as well as of the buyers and

sellers who participate in commerce on the website. The website was designed to achieve this anonymity primarily by operating as a hidden service on the Tor network.

c. To further promote anonymity, purchases were made primarily in bitcoin (or other virtual currency) using Nucleus's escrow services, i.e., a buyer transferred funds from his or her own account or virtual-currency wallet into an Nucleus account or wallet, and Nucleus subsequently transferred the funds to the seller's account or wallet upon satisfaction of the terms of sale. In doing so, Nucleus also provided a "tumbling" or "mixing" service which essentially scrambled multiple buyer-seller Bitcoin transactions together in order to conceal the bitcoin payments from buyer to seller or commission payments to the administrator. Thus, there was no direct bitcoin transaction between the buyer and the seller.

25. On April 13, 2016, Nucleus went offline for an unknown reason. At this time, there are over 5000 bitcoins, currently valued at $3.6 million, still contained within Nucleus bitcoin wallets. The true identity of the individual or individuals who controlled and operated the Nucleus website, *i.e.*, the administrator(s), is unknown.

D. "POLIRA" Vendor on Nucleus Market

26. Since at least September of 2015, agents identified a narcotics vendor, known as "POLIRA," appearing on the Nucleus Market. (Law enforcement had previously identified "Kevin Fusco" as using the name "Polira" to purchase MDMA on the dark web based on information obtained from the seized website servers of the now defunct criminal dark web marketplaces Silk Road and Silk Road 2.0.)

27. On several occasions, DEA agents have made undercover online purchases of MDMA from "POLIRA" and received the MDMA via U.S. Mail, shipped to undercover mailboxes in Miami, Florida. For instance:

a. On October 14, 2015, DEA agents purchased 1 gram of MDMA from "POLIRA" on the Nucleus Marketplace for 0.2749 bitcoins. In the description, POLIRA stated: "1 Gram MDMA - Lab Tested 88% pure!;" and,

b. On November 17, 2015, DEA agents purchased 25 MDMA pills from "POLIRA" on the Nucleus Marketplace for 5.875 bitcoins. In the description, POLIRA stated: "5 Yellow Snapchat - 220mg MDMA."

28. In both instances, the controlled substances were shipped via United States Priority Mail with New York City return addresses. Laboratory results have confirmed the items received in Miami, Florida, contained MDMA.

29. Based on "POLIRA's" profile on Nucleus, as well as vendor reviews on various internet forums, "POLIRA" has conducted hundreds of transactions on at least two Dark Web marketplaces, including: Nucleus with at least 492 transactions and Agora with an undetermined number of transactions. On both marketplaces, "POLIRA" advertised MDMA.

E. FUSCO & Fusco Residence Associated with "POLIRA"

30. Since the time of the first controlled purchase from "POLIRA" on October 14, 2015, DEA and other law enforcement agents have been able to confirm the identity FUSCO as the "POLIRA" on Nucleus using the shipping records associated with the packages of drugs shipped to DEA via the United States Postal Service (USPS)

31. USPS records revealed that the aforementioned undercover drug purchase November 17, 2015 was shipped using postage purchased at "Stamps.com".

32. Records obtained from Stamps.com revealed that the Stamps.com account used by "POLIRA" to ship the drugs to UC agents was opened in January of 2014 and registered under the name of "Kevin Fusco" and address 226 E 14th Street, Apartment 4R, New York, New York

10003. A search of New York Department of Motor Vehicles database revealed that FUSCO resides at 226 E 14th Street, Apartment 4R, New York, New York 10003 (hereinafter, the "Fusco Residence").

33. FUSCO's Stamps.com account further revealed that between January 2014 and August 2016, approximately $29,093.17 in postage was purchased and used for approximately 5,263 individual mailings and packages, dozens of which were shipped to addresses in the Southern District of Florida. In addition, Stamps.com IP connection records revealed logins into FUSCO's Stamps.com account from IP addresses belonging to Time Warner Cable. Records from Time Warner Cable revealed the Stamps.com login IPs were assigned to FUSCO at the exact dates and times that the IPs were captured by the Stamps.com system, and that FUSCO subscribed to wireless internet service with service address at the Fusco Residence.

34. FUSCO's Stamps.com IP connection records also reveal that on November 15, 2015, Stamps.com captured a login IP address belonging to the Tideline Resort in Palm Beach, Florida. A subpoena to Tideline Resort revealed that FUSCO stayed at the resort from November 14, 2015 to November 16, 2015.

35. In addition, the Stamps.com records revealed that FUSCO shipped his packages from the New York area and that during the time period that FUSCO stayed at the Tideline Resort in Florida, there was no shipping inactivity. Similarly, FUSCO's Stamps.com account showed shipping inactivity from February 22, 2016 to March 28, 2016, coinciding with a time that FUSCO is known to have been travelling overseas, based U.S. immigration records.

F. Tor Network Activity from the Fusco Residence

36. In order to determine whether FUSCO, and/or some other narcotics-trafficking co-conspirator, was accessing criminal, Dark Web marketplaces from the Fusco Residence, law

enforcement began monitoring the internet traffic to and from the IP address associated with the Fusco Residence.

37. As discussed above, because of the anonymity provided by the Tor network such monitoring would not reveal the ultimate IP address of devices communicated with through the Tor network. However, such monitoring could reveal connections to computers generally associated with the Tor network as relays (or "Tor Nodes") which are the computers and servers designated by the administrators of the Tor network to route communications through the encrypted Tor network.

38. For example, monitoring the IP connections of a computer connecting to Nucleus through Tor, will not reveal any specific IP address associated with Nucleus. Rather such monitoring could[4] reveal connections to computers generally associated with the Tor network as "Tor Nodes," which are the computers and servers designated by the administrators of the Tor network to route communications through the encrypted Tor network.

39. A computer attempting to connect to the Tor network must know how to contact a Tor Node in order to initiate a Tor network session, and Tor Node IP addresses are publicly available, open source information on websites such as: https://exonerator.torproject.org.

40. Therefore, monitoring the traffic of the IP address of someone suspected of using the Tor network could reveal connections to IP addresses publicly associated with computers and servers known to operate as Tor Nodes.

---

[4] This would not necessarily be the case if the person was adding an additional layer of anonymity, such as a virtual private network (VPN) connection, between them and the Tor network.

41. On January 25, 2017, the DEA obtained a pen/trap order for all internet traffic to and from the Comcast IP addresses associated with the Fusco Residence. The pen/trap order results obtained through February 20, 2017 reveal numerous internet connections from the Fusco Residence IP address to known Tor Nodes and, therefore, the Tor network, which is consistent with someone logging on to criminal Dark Web marketplaces through the Tor network, from a computer located within Fusco Residence.

G. Financial Analysis

42. Law enforcement was able to identify a Coinbase bitcoin account used by the Silk Road 2.0 user "Polira." Coinbase account records, revealed that the account was opened on April 2, 2013 in order to buy and sell bitcoins in FUSCO's name, and listing the Fusco Residence as his home address, and an email and phone number also known to be FUSCO's.

43. Records from this account link it to several bank accounts in FUSCO's name and show that FUSCO received and cashed out bitcoin valued at over $200.,000 from October 2, 2013 through July 22, 2015.

44. Law enforcement also identified bitcoin cash out transactions conducted and attempted by FUSCO with Cottonwood Vending LLC which operates a network of automated bitcoin teller machines, *i.e.*, ATM machines which provide cash for bitcoin. Cottonwood Vending records show that from October 28th, 2015 through December 15th, 2015 FUSCO utilized a Cottonwood bitcoin ATM machine located at Good Guy Vapes smoke shop at 23 Cleveland Place, New York, New York to conduct numerous bitcoin sale transactions in exchange for U.S. currency for a total of $32,280.00. During the ATM transactions, FUSCO provided a copy of his New York driver license with the address listed as the Fusco Residence.

45. On December 15, 2015, FUSCO attempted to cash out more than $200,000 at a Cottonwood ATM from bitcoin wallet 17yXgax9edSo6rgycJ1KMrKMFTu3bvRwdG (hereinafter "Wallet 17yXgax"). Cottonwood ultimately rejected the transaction because it could not verify a legitimate source of funds.

46. Forensic analysis of the bitcoin flowing into Wallet 17yXgax revealed that 68.71% of all bitcoin received into his wallet originated from Dark Web market sites. Specifically, from approximately November 16, 2014 through December 15, 2015 a total of 1,535 bitcoin was sent directly from three Dark Web market sites known as Agora, Evolution, and Nucleus Market to wallet 17yXgax.

47. Based on my training and experience I know that criminal dark web vendors often seek to cash out the bitcoin they receive from their illicit activities, in order to spend and enjoy the proceeds, and often attempt to do so with various and ever changing methods.

CONCLUSION

48. Based on the foregoing, probable cause exists that:

a. Kevin FUSCO, did, at least from October 14, 2015 through April 13, 2016, conspire with the unknown administrator(s) of Nucleus, to distribute controlled substances, including MDMA, in violation of Title 21, United States Code, Sections 846 and 841(b)(1)(c);

b. Kevin FUSCO, did, at least from October 14, 2015 through April 13, 2016, conspire with the unknown administrator(s) of Nucleus, to knowingly conduct financial transactions, in bitcoins, involving the proceeds of unlawful narcotics trafficking activities, knowing that the transaction was designed to conceal and disguise the nature of the proceeds, in violation of Title 18, United States Code, Section 1956(h) and 1956(a)(1).

Respectfully submitted,

MARIA ISABEL VASALLO, SPECIAL AGENT
DRUG ENFORCEMENT ADMINISTRATION

The contents of this written affidavit were subscribed and sworn before me on March 9, 2017.

HONORABLE BARRY L. GARBER
UNITED STATES MAGISTRATE JUDGE