UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

No. 17-mj-03241-JG

UNITED STATES OF AMERICA

v.

GAL VALLERIUS,
a/k/a, "OXYMONSTER,"

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,

BENJAMIN G. GREENBERG
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.

GAL VALLERIUS, a/k/a, "OXYMONSTER,"

Defendant(s)

Case No. 17-mj-03241-JG

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 3/2015-8/2017 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)(a)	Conspiracy to Distribute Controlled Substances

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

Complainant's signature

Austin D.Love, S/A, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: Aug 31, 2017

Judge's signature

City and state: Miami, Florida

Jonathan Goodman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, AUSTIN D. LOVE, Special Agent with the Drug Enforcement Administration (DEA), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. This application in furtherance of an investigation worked jointly with the Federal Bureau of Investigations (FBI), the Internal Revenue Service (IRS), Homeland Security Investigations (HSI), and the United States Postal Inspection Service (USPIS).

2. 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, Sections 846 and 878.

3. This affidavit is made in support of a criminal complaint charging Gal VALLERIUS, a/k/a, "OxyMonster," with conspiracy to distribute in narcotics in violation of Title 21, United States Code, Section 846.

4. 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.

5. 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

6. This application stems from an ongoing criminal investigation into drug dealers operating on criminal online marketplace websites, including a website known as Dream Market. In the course of this investigation, I have learned that the Dream Market website is one of many The Onion Router ("Tor") network or "dark web" criminal marketplaces. Dream Market is 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, probable cause exists that VALLERIUS, acted as an Administrator, Senior Moderator and Vendor on Dream Market, playing a critical role in supporting daily illicit transactions between buyers and vendors on Dream Market, such as the trafficking in narcotics and laundering in the proceeds of their activities using the Bitcoin and the dark web, in conspiracy with additional known and unknown administrator(s), moderators, and vendors of the Dream Market.

A. 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.

---

[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.

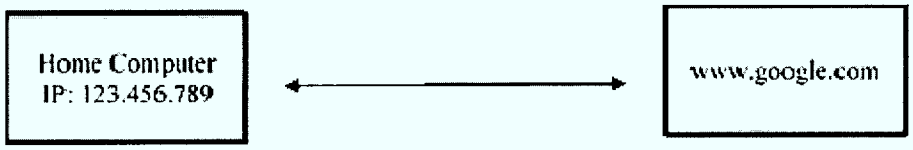
[2] Private individuals operating home computers usually do not own and register their own IP address; instead, they subscribe to broadband accounts with ISPs, such as Comcast or AT&T, which in turn assign or lease an IP address to them (the subscriber). Nevertheless, the IP address can usually be traced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

B. 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 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.

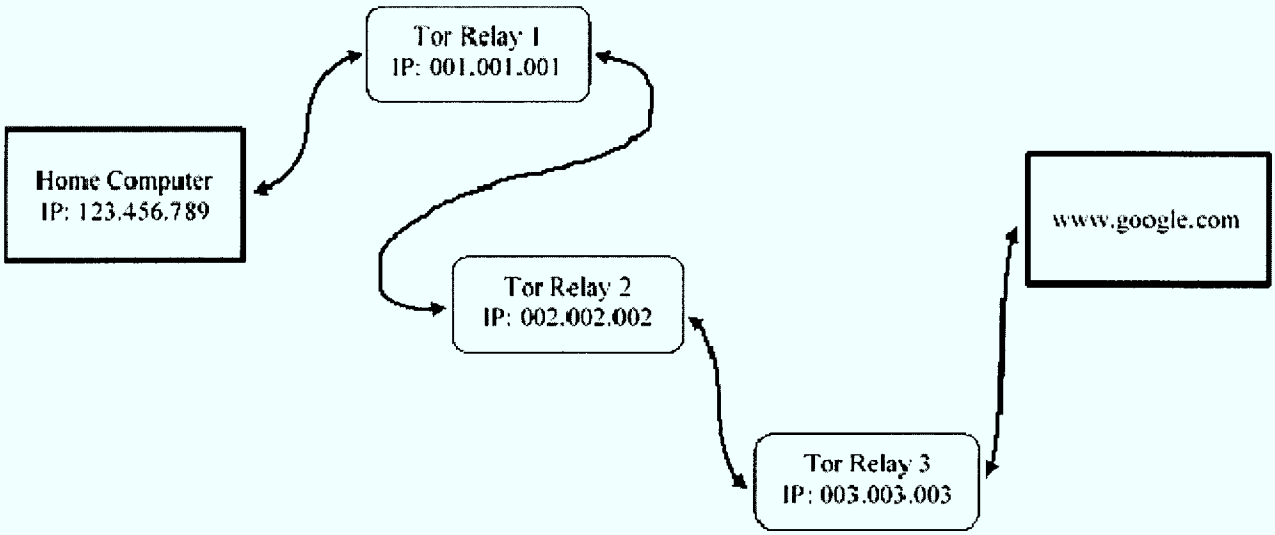
14. By way of illustration, in a standard internet communication, when a person connects to a website, that website can see that persons IP address:



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."

C. 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]

D. Description of the Dream Market Narcotics Distribution Conspiracy

23. Dream Market provides an infrastructure that allows buyers and sellers to conduct transactions online, in a manner similar to well-known online marketplaces such as eBay. Like eBay:

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

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

c. Dream Market charges a commission from every transaction as a percentage of the sale price.

24. However, unlike legitimate online marketplaces, Dream Market is dedicated and designed to facilitate the sale of illegal narcotics and drug paraphernalia. For example:

a. Illegal drugs, such as methamphetamines, heroin, and cocaine, are openly advertised and sold and are immediately and prominently visible on the Dream Market website.

---

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

b. The Dream Market website is 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 is designed to achieve this anonymity primarily by operating as a hidden service on the Tor network.

c. To further promote anonymity, purchases are made primarily in bitcoin (or other virtual currency) using Dream Market's escrow services, i.e., a buyer transfers funds from his or her own account or virtual-currency wallet into an Dream Market account or wallet, and Dream Market subsequently transfers the funds to the seller's account or wallet upon satisfaction of the terms of sale. In doing so, Dream Market also provides a "tumbling" or "mixing" services which essentially scrambles 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 is no direct bitcoin transaction between the buyer and the seller.

25. As of August 29, 2017, there are a total of 94,236 listings on Dream Market, to include the following categories:

a. "Drugs" (47,405 listings). The "Drugs" category is broken down into the following sub-categories: Stimulats, Opioids, Ecstasy, Cannabis, Barbituates, Benzos, Cannabis, Dissociatives, Prescription, Psychedelics, RCs, Steroids and Weight Loss. Each sub-category contains different types of controlled substances, such as heroin, fentanyl, methamphetamine and cocaine. For example, the "Stimulats" category contains 934 listings for crystal methamphetamine ranging from .5 grams to 11 pounds per listing, totaling over 200 pounds of crystal methamphetamine at any given time.

b. "Digital Goods" (41394 listings). The "Digital Goods" category is broken down into the following sub-categories: Data, Drugs, E-Books, Fraud, Fraud Related, Hacking, Information, Other, Security, Software.

c. "Drug Paraphernalia" (456 listings).

d. Services (3056 listings). The "Services" category is broken down into the following sub-categories: Hacking, IDs & Passports, Money, Other, Cash out.

e. "Other" (2382 listings). The "Other Category" is broken down into the following sub-categories: Counterfeits, Electronics, Jewelry, Lab Supplies, Miscellaneous and Defense.

26. These activities and the marketplace website itself is overseen, managed and controlled by Dream Market administrator(s) and moderators in conspiracy with each other and all of the vendors on the marketplace.

a. Dark Web marketplace administrators typically create, modify, maintain, and control the actual website and the sever on which its located, as well as ultimately control the activity among the marketplace's participants, including the appointment of moderators and other to help in that roll.

b. Moderators typically moderate disputes between the marketplace's vendors and buyers and seek to assure the continued operation of its activities.

27. The true identity of the all of the individuals who currently control and operate on the Dream Market website as administrators, moderators or vendors is unknown.

E. Dream Market: Drug Distribution & Venue in Southern District of Florida

28. Since at least February of 2016, agents identified narcotics vendors operating on Dream Market under the following monikers: Digitalpossi2014, ReximusMaximus and

MethForDummies. On several occasions, DEA agents have made undercover online purchases of crystal meth, LSD and hydrocodone from the aforementioned vendors on Dream Market and received the drugs via U.S. Mail, shipped to undercover mailboxes in Miami, Florida. For instance:

a. On February 25, 2016, DEA agents purchased 100 sheets of LSD from ReximusMaximus on Dream Market for 1.084 bitcoins. In the description, ReximusMaximus stated: "100X GDF 150ug LSD!!";

b. On May 25, 2016, DEA agents purchased one hydrocodone pill from Digitalpossi2014 on Dream Market for 0.0993 bitcoins. In the description, Digitalpossi2014 stated "(ONE) 10.325 Hydrocodone 14.50 a piece."

c. On May 25, 2016, DEA agents purchased 10 hydrocodone pills from Digitalpossi2014 on Dream Market for 0.2207 bitcoins. In the description, Digitalpossi2014 stated, "(TEN) 7.5 Hydrocodone $100.00 free 2/3 day priori."

d. On May 25, 2016, DEA agents purchased 28 grams of crystal methamphetamine from MethForDummies on Dream Market for 1.516 bitcoins. In the description, MethForDummies stated, "MFD's HQ crystal methamphetamine 28 grams."

29. In all four instances, the controlled substances were shipped via United States Priority Mail to Miami, Florida. Laboratory results confirmed that the above-listed items contained controlled substances, including LSD, hydrocodone, and crystal methamphetamine.

F. "OxyMonster" Administrator, Senior Moderator & Vendor on Dream Market

30. On January 27, 2017, DEA agents logged into Dream Market and observed a link to "Forum" on the Dream Market home page. Agents clicked on the link, which took them to a Tor website called Dream Market Forum. Based on my training and experience, dark web market

administrators create forum webpages on the dark web to allow vendors, buyers and administrators to discuss anything related to the dark web market. In order to post on the forum, one must create a profile with a username and password, anyone can join the forum, but only a Dream Market, administrator, moderator or vendor, verified by the Dream Market administrators will appear marked as an "administrator," "moderator" or "vendor" on the forum.[4] Unverified forum users are marked as "members".

31. While browsing the Dream Market Forum, agents navigated to a topic called "[[[OFFICIAL STAFF]]]" under the "Announcements" tab. The first posting was written on July 23, 2016 by user "OxyMonster." The posting stated:

> *Anyone that's claiming to Mod or Admin who's not on this list – should be reported immediately.*
> ***Admin:*** *SpeedStepper*
> ***Senior Moderator:*** *OxyMonster*
> ***Moderators:*** *Quasimodo, FriedTheChicken*
> ***Ticket conductors:*** *Xray, SpanishConnect"*
> *Senior Moderator @ Dream market Ichudifyeqm4idjj.onion/?al=55781*

32. The user "OxyMonster's" title was marked as Senior Moderator. Agents clicked on the user "OxyMonster" and were taken to "OxyMonster's" profile on Dream Market. The profile stated that "OxyMonster's" was a Senior Moderator on Dream Market, whose profile was registered on the Dream Market Forum on May 10, 2015.

33. Several months later, on June 30, 2017, agents also identified "OxyMonster" as a vendor on Dream Market. "OxyMonster's vendor profile featured listings for Schedule II

[4] On the Dream Market Forum, whenever a user posts a comment, his/her username is displayed next to the comment. Also, next to the username, a user is identified as a Dream Market vendor, moderator, administrator, or member. All vendors, moderators and administrators have to be verified as such by the Dream Market administrator(s). Unverified Dream Market users are marked as members.

controlled substances OxyContin and Ritalin. His profile listed 60 prior sales and five star reviews from buyers. In addition, his profile stated that he ships from France to anywhere in Europe. Under the "Terms and Conditions" section, his profile stated,

We highly recommend using TradeRoute for purchasing from us:
Trade routeilbgzt.on ion/?shop=OxyMonster..."
THE OFFICIAL TIP JAR FOR "DREAM TEAM" (STAFF) IS:
1DREAMv7k16T8bMyE7ghe4nLQVydBbPJAe.

34. Agents navigated to the aforementioned TradeRoute link, which led them to OxyMonster's drug vendor page TradeRoute—an emerging dark web marketplace similar to Dream Market. OxyMonster's TradeRoute profile stated that he was an active drug vendor, who ships from France to Europe and the United States and has been a member since February, 2017. In addition, his profile stated:

YES, we were mods on Evo
YES, we were admins on Dream

35. In other posts on the Dream Market forum, "OxyMonster" characterized himself as a Dream Market administrator. For instance, on December 10, 2015, "OxyMonster" posted the following:

Being promoted is always nice, especially once hitting the "Admin" role.
That being said, we will be focusing more on the market's aspects obviously.

36. On August 28, 2017, agents once again logged into the Dream Market forum and viewed "OxyMonster's" profile. At that time, his title was changed to "Vendor" on Dream Market. His profile also stated that he has 1,052 posts and his last post was on February 13, 2017. In addition, he had a signature, which stated:

*Senior Moderator @ Dream market Ichudifyeqm4idjj.onion/?ai=55781" * REAL DREAM STAFF TIP JAR: 1DREAMv7k16T8bMyE7ghe4nLQVydBbPJAe.*[5]

37. Agents reviewed all of "OxyMonster's" posts on the Dream Market Forum, which began on May 10, 2015 and ended on December 22, 2016. "OxyMonster's" posts responded to customer complaints, provided tips on staying anonymous on the dark web and posted the names of the official staff of Dream Market.

38. On August 29, 2017, agents viewed "OxyMonster's" Dream Market vendor profile. This time, the vendor profile stated that he will also ship to the United States. The vendor profile now had 70 verified sales and still listed the same Dream Market staff tip jar bitcoin wallet and he was last online on August 29, 2017.

39. In sum, "OxyMonster" knowingly participated the Dream Market conspiracy not only as a vendor, but also, in a leadership and organizational roll as a senior moderator and administrator.

F. Gal VALLERIUS Identified as "OxyMonster"

40. After observing the bitcoin "tip jar" advertised by "OxyMonsyter," agents conducted analysis of the incoming and outgoing transactions from that bitcoin address and learned that 15 out of 17 outgoing transactions from the "OxyMonster" tip jar went to multiple wallets controlled by French national Gal VALLERIUS on Localbitcoins.com.

41. Open source data revealed that VALLERIUS has Instagram and Twitter accounts. Agents compared the writing style of "OxyMonster" on Dream Market forum while in Senior

---

[5] Based on my training and experience, a bitcoin "tip jar," is utilized by dark web market vendors and administrators to receive tips in bitcoin for their service from the users of the dark web market.

Moderator role to the writing style of VALLERIUS on his public Instagram and Twitter accounts. Agents discovered many similarities in the use of words and punctuation to including: the word "cheers;" double exclamation marks; frequent use of quotation marks; and intermittent French posts.

42. On August 31, 2017, VALLERIUS travelled to the United States for the first time to attend an international beard competition in Austin, Texas. A border search of his laptop upon his arrival at Atlanta International Airport confirmed his identity as "OxyMonster." On his laptop was the TOR browser, apparent log-in credentials for Dream Market, $500,000 worth of bitcoin, and a PGP encryption key[6] entitled "OxyMonster" which matched that advertised as "OxyMonster's" on Dream Market.

---

[6] Persons who are involved with Dark Web narcotics trafficking utilize public key encryption to communicate with other purchasers and sellers on the marketplace in order, for instance, to provide information such as a shipping address. If the message was not encrypted, it would be visible by the administrators of the Dark Web marketplace, and by law enforcement, if the marketplace server was ever located and seized. Public key encryption allows the sender of a message to encrypt that message using a long and unique passcode known as a public key, which the recipient of the message publicly provides to anyone wishing to communicate with them. That message, in turn, can only be decrypted by the recipient using a corresponding private key known only to them. The most commonly used encryption is that known as Pretty Good Privacy (PGP) encryption. Almost all Dark Web marketplace vendor profiles advertise a public PGP key for this purpose; the PGP key, therefore, doubles as a unique fingerprint visible across dark web platforms.

CONCLUSION

43. Based on the foregoing, probable cause exists that Gal VALLERIUS, did, at least from May 2015 to August 2017 conspire to distribute controlled substances, including cocaine, fentanyl, methamphetamine, LSD, and oxycodone in violation of Title 21, United States Code, Section 846.

Respectfully submitted,

AUSTIN D. LOVE, SPECIAL AGENT
DRUG ENFORCEMENT ADMINISTRATION

The contents of this written affidavit were subscribed and sworn before me on August 31, 2017.

JONATHAN GOODMAN HONORABLE
UNITED STATES MAGISTRATE JUDGE