

UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America)
v.)
MARCOS PAULO DE OLIVEIRA-) Case No.
ANNIBALE,)
aka "Med3lin,")
aka "Med311n,")
aka "Med311n_WSM")
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 October 2017 through April 2019 in the county of Sacramento in the Eastern District of California, and elsewhere, the defendant(s) violated:

Code Section Offense Description
21 U.S.C. §§ 841 and 846 Distribution and Conspiracy to Distribute Controlled Substances
18 U.S.C. §§ 1956 and 1957 Money Laundering

This criminal complaint is based on these facts:

(see attachment)

[X] Continued on the attached sheet.

Jay D Dial Jr JDR
Complainant's signature

JAY D. DIAL, Jr., Special Agent
Drug Enforcement Administration
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/2/14

Allison Claire
Judge's signature

City and state: Sacramento, CA

Allison Claire, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America)
v.)
MARCOS PAULO DE OLIVEIRA-) Case No.
ANNIBALE,)
aka "Med3lin,")
aka "Med311n,")
aka "Med311n_WSM")
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 October 2017 through April 2019 in the county of Sacramento in the
Eastern District of California, and elsewhere, the defendant(s) violated:

Code Section Offense Description
21 U.S.C. §§ 841 and 846 Distribution and Conspiracy to Distribute Controlled Substances
18 U.S.C. §§ 1956 and 1957 Money Laundering

This criminal complaint is based on these facts:
(see attachment)

[X] Continued on the attached sheet.

JAY D. DIAL, Jr., Special Agent
Drug Enforcement Administration
Printed name and title

Sworn to before me and signed in my presence.

Date: 5-2-19

Allison Claire
Judge's signature

City and state: Sacramento, CA

Allison Claire, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Jay D. Dial, Jr., being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent (SA) with the Drug Enforcement Administration (“DEA”) since May 2005 and am presently assigned to the DEA's District Office in Fresno, California. I successfully completed a 16-week Basic Agent Training Academy at the DEA Academy in Quantico, Virginia. This training included instruction in the investigation of federal drug violations, including, but not limited to, Title 21, United States Code, Sections 841 and 846. Additionally, I have discussed with numerous law enforcement officers, defendants, and informants, the methods and practices used by narcotics distributors, including those who use the Internet to distribute narcotics. I have also been the affiant of previous federal and state search warrants and have testified in court about narcotics.

2. Further, I have completed various training programs provided by the DEA and local law enforcement agencies, including training on identifying characteristics associated with the manufacture, sale, and transportation of various narcotics, including methamphetamine, heroin, cocaine, and marijuana. These training programs involved the use, possession, packaging, sale, concealment, manufacturing, and transportation of various controlled substances as well as its precursors and chemicals used in the manufacturing process. I am familiar with narcotics traffickers' methods of operation including the distribution, storage, manufacturing, and transportation of narcotics, and the collection of money proceeds of narcotics trafficking. I have assisted on the execution of several federal and state narcotics search warrants that resulted in the arrest of suspects and seizure of narcotics.

3. I have participated in other narcotics investigations, either as a case agent or in a supporting role. I also have debriefed defendants, informants, and witnesses who had personal knowledge regarding narcotics trafficking organizations. Additionally, I have participated in many other aspects of drug investigations including, but not limited to, undercover operations, conducting physical and electronic surveillance, and arrests. These investigations have included

the unlawful manufacture, possession, distribution, and transportation of controlled substances, as well as conspiracies associated with criminal narcotics, in violation of Title 21, United States Code, sections 841(a)(1), 841(c)(2), 843, and 846.

4. I have also attended Darknet and virtual currency conferences. I have participated in investigations that targeted heroin and fentanyl vendors operating on the Darknet, specifically on AlphaBay and Wall Street Market. Additionally, I was a case agent on the investigation and takedown of AlphaBay, which at the time was the world's largest Darknet marketplace. As a result of these investigations, I have obtained experience in purchasing the virtual currency, such as Bitcoin, and conducting undercover purchases of narcotics through Darknet markets, and I have learned various techniques to identify vendors and other users of Darknet markets. I have also learned how virtual currency is used to launder funds and to facilitate the purchase of illegal goods on Darknet markets. In addition to my own experience and training, I have relied on the training and experience of other agents who have significant expertise in Darknet and other cybercrime-related investigations.

5. I make this affidavit in support of an application for a criminal complaint against **MARCOS PAULO DE OLIVEIRA-ANNIBALE** (hereafter "ANNIBALE"). As described more fully below, I respectfully submit there is probable cause to believe that ANNIBALE has committed violations of 21 U.S.C. §§ 841 and 846 (Distribution and Conspiracy to Distribute Controlled Substances) and 18 U.S.C. §§ 1956 and 1957 (Money Laundering).

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested criminal complaint and arrest warrant 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.

II. RELEVANT DEFINITIONS

7. Based upon my training, experience, and research, I know that:

a. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state.

b. Individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, and other information both in computer data and written record format.

c. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178), or a series of eight groups of four hexadecimal digits, with the groups separated by colons (e.g., 2001:0db8:0000:0042:0000:8a2e:0370:7334). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

d. When a customer logs into the Internet using the service of an ISP, the computer used by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period.

e. Tor is an anonymous proxy network on the Internet. Individuals who use Tor generally can remain anonymous to the destination server by routing their Internet traffic through the Tor network. Tor is made up of a decentralized network of computers or "nodes," which relay traffic anonymously from the source node (i.e., the computer sending data), to the destination node (i.e., the computer receiving data). When Tor is used as an intermediary to route data, the path that the data can take is completely random, and the number of nodes that the data goes through before reaching the destination can vary. The nodes that relay the data within the Tor network from the source to the destination are called "relay nodes," while the final node in the Tor network, which sends the data to the destination computer, is called an "exit node." The data is encrypted from the time it leaves the source node, until it leaves the exit node and is finally forwarded to the destination computer. Tor requires that specialized software be downloaded and installed on the source node (i.e., the target's computer) to allow the data sent from the source node to be routed through the Tor network. Once the Tor software is installed, other Internet software on the source node computer (for example, a web browser) must be configured to use Tor, and thus to remain anonymous. The Tor network is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true 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" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the Tor network.

f. "Darknet" or "Darkweb" refers generally to network(s) not accessible on the "surface web," which is what the layperson understands to be the Internet. Specifically, darknet websites (such as Silk Road, an infamous darknet market) operate on the Tor network.

g. Through the dark web or "darknet," i.e., websites accessible only through anonymity-enhancing networks such as Tor, individuals have established online marketplaces,

such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through virtual currencies, such as Bitcoin. These markets usually have escrow accounts, through which consumers deposit their virtual currency for an order placed on the marketplace; the funds are released to the vendor upon acknowledgement from the consumer that the good(s) purchased have been received. The escrow account then accepts a fee for each transaction, which in turn goes to the operator of the darknet marketplace and serves as a commission and/or payment for the operation of the darknet marketplace.

h. Darknet marketplaces are often organized in a hierarchical manner. At the top of the organization's hierarchy are the "administrators," responsible for developing the site and keeping its content and design backed up and fully functional. The administrators are also often the individuals with access to the site's servers and databases, and also have control over the site's virtual currency wallets. Under the administrators of a site are its "moderators," employees responsible for resolving disputes between vendors and customer. Darknet marketplaces also often employ public relations specialists, who promote the site through other websites. Administrators and other employees of Darknet marketplaces are often paid through the fees charged to vendors and customers for each transaction.

i. Darknet marketplaces usually exist for finite periods of time. Over the past few years, law enforcement has seized certain marketplaces, such as the Silk Road, AlphaBay, and Hansa. Accordingly, operators of Darknet marketplaces take steps to avoid law enforcement detection.

j. Virtual 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). Virtual 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. Virtual currency is not illegal in the United States and may be used for legitimate financial transactions. However, virtual currency is often used for conducting illegal transactions, such as the sale of controlled substances.

k. Bitcoin is a type of virtual currency. Bitcoin payments are recorded on a public ledger (known as the “Blockchain”) that is maintained by peer-to-peer verification, and is thus not maintained by a single administrator or entity. Individuals can acquire bitcoin either by “mining” or by purchasing bitcoin from other individuals. An individual can “mine” for bitcoin 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 bitcoin.

l. An individual can send and receive bitcoin 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.

m. Bitcoin are stored in (or accessed through) digital “wallets.” A digital wallet stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. Many companies offer wallet services, such as Coinbase, Copay, and Blockchain. 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. Bitcoin transactions are, therefore, described as “pseudonymous.”

n. PGP is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting text, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PGP was developed by a software engineer in 1991 who wanted a way to transfer information securely over the Internet. Today, PGP is implemented throughout the public and private sector to help secure sensitive data transfers and communications.

o. PGP encryption has multiple uses. It can be used in conjunction with a user’s email account, and for message authentication and integrity checking. However, PGP’s most common use is to incorporate it with an email account, through which PGP provides the means for users to encrypt and decrypt messages. Email addresses that are associated to a PGP

key pair are likely to contain communications that the PGP protocol used to encrypt and decrypt messages. PGP in its most simplistic form consists of a person using a PGP tool to create a PGP key pair. The PGP key pair contains both a public key (to lock/encrypt the message) and a private key (to unlock/decrypt the message). In the event a person wants to send a secure message to a friend, that person would send his/her public key to the friend, in which the friend could then encrypt a sensitive message and send it back encrypted. The person receiving the sensitive message would then decrypt the message with his/her private key.

III. SUMMARY OF PROBABLE CAUSE

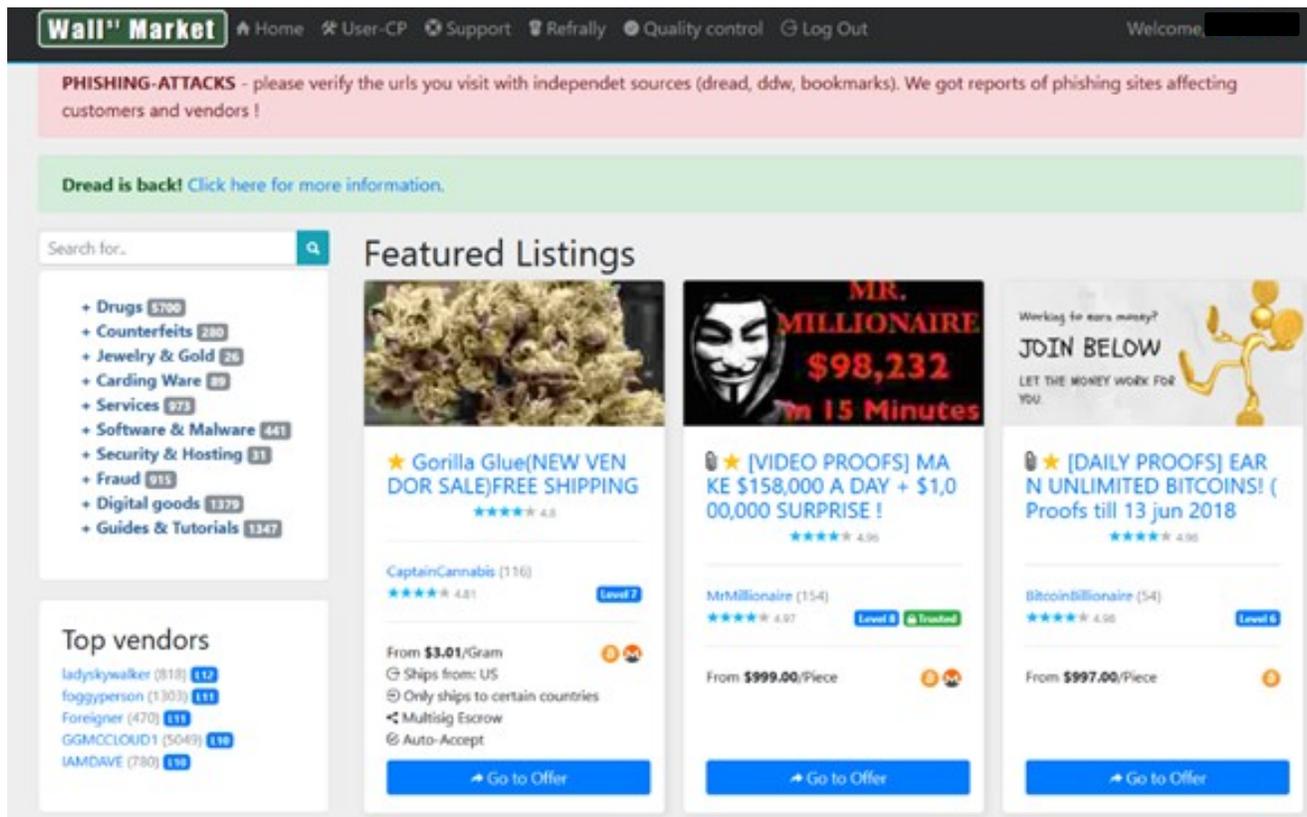
8. In or around July of 2017, the DEA, in conjunction with the FBI and other federal investigative agencies, including Homeland Security Investigations (“HSI”) and the Internal Revenue Service (“IRS”), began an investigation into Wall Street Market (“WSM”), a Darknet marketplace known to host the trafficking of illegal narcotics, hacking tools, stolen financial data, and other contraband through the Internet (Tor) and the United States mail. As part of this investigation, as more fully described below, law enforcement has identified **MARCOS PAULO DE OLIVEIRA-ANNIBALE**, aka “Med3Lin,” aka “Med3L1N,” aka “Med3L1N_WSM,” as a moderator of the marketplace, i.e. an employee with managerial responsibility, including resolving disputes on narcotics transactions between vendors and consumers, and the promotion of the site on public Internet forums.

IV. STATEMENT OF PROBABLE CAUSE

A. Background on Wall Street Market

9. From approximately 2016 to 2019, as described herein, WSM was a Darknet marketplace where vendors advertised and marketed the sale of illegal narcotics, malicious software, stolen financial data, counterfeit goods, and more. Indeed, as of April 22, 2019, WSM was one of the largest and most voluminous Darknet marketplaces of all time, made up of approximately 5,400 vendors and 1,150,000 customers around the world, as advertised and posted on the WSM homepage. As described more fully below, WSM has been placed in “Maintenance Mode” by German authorities (and therefore is non-operational). Further, German

authorities have arrested the three suspected administrators of the site, who as recently as April 2019, are believed to have conducted an “exit scam.” As background, an “exit scam” is when the administrators of a Darknet marketplace shut it down and take all of the virtual currency held in the marketplace escrow and user accounts.



10. WSM operated like a conventional e-commerce website, such as eBay and Amazon. However, its features are geared to the trafficking of contraband. Based on the other case agents of WSM, including as an undercover consumer and vendor, I am aware of the following:

- a. WSM was a “hidden service,” that is, on the dark net, accessible only by programs such as Tor.
- b. WSM’s interface was available in six different languages: English, German, Spanish, French, Portuguese, and Italian.

c. WSM buyers were required to register for a free account by selecting a unique user name (otherwise known as a moniker) and password. Once an account was created, users were able to browse goods for sale from the home page, which were organized by specific categories. Some of the categories include “Drugs,” “Counterfeits,” “Jewelry & Gold,” “Carding Ware,” “Services,” “Software & Malware,” “Security & Hosting,” “Fraud,” “Digital Goods,” and “Guides & Tutorials.”

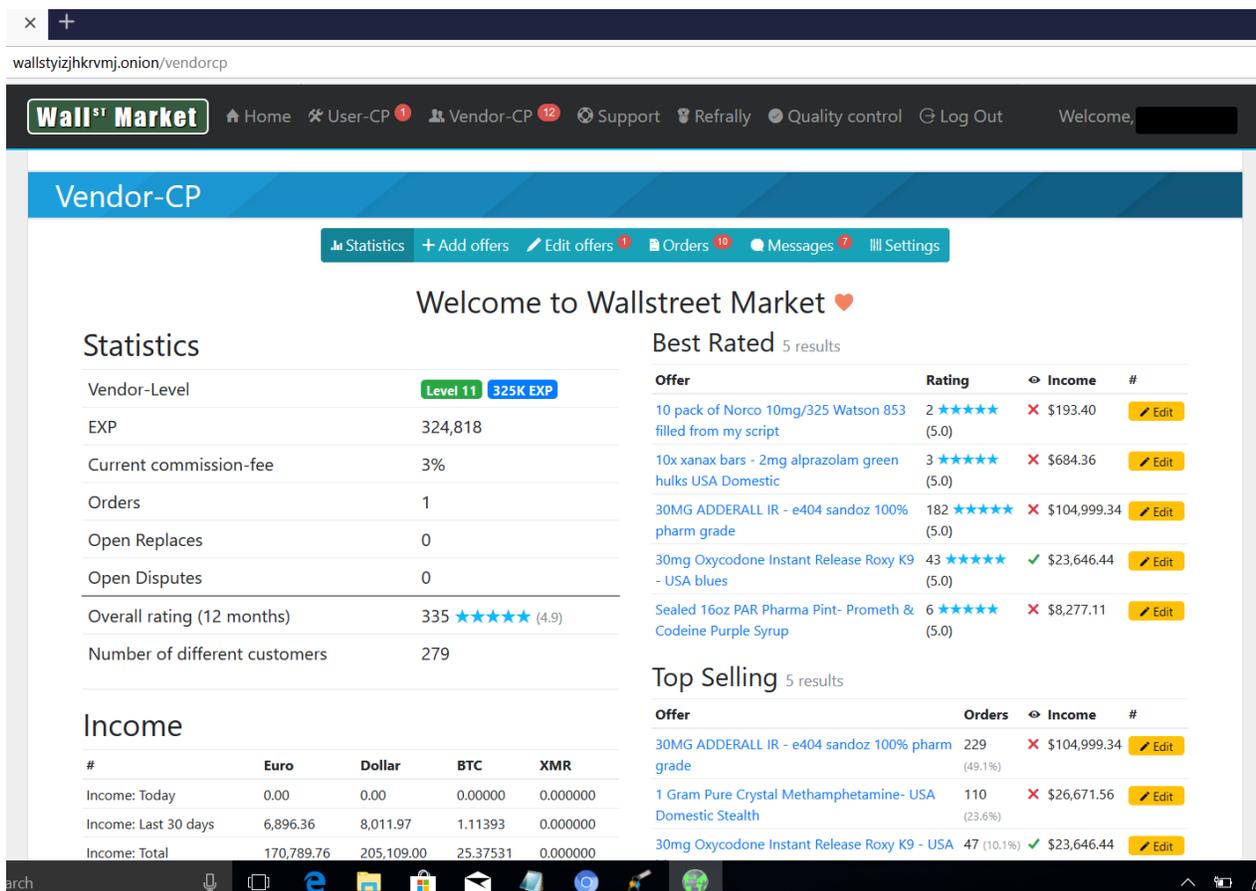
d. WSM buyers were able to make purchases of contraband on WSM and usually received physical contraband through the United States Mail and/or other means of physical delivery, such as commercial courier.

e. WSM also provided a search function that allowed users to locate listings for the types of illegal goods or services they would want to purchase, and permitted searching by price range, popularity of item, vendor ratings, origin or shipping country, and payment type. WSM also operated a forum (“the WSM Forum”) for users to discuss WSM-related matters. The forum was maintained and operated by moderators, whose responsibilities included responding to any questions regarding WSM among other things.

f. WSM required its users to trade in virtual currencies, including Bitcoin and Monero, and did not allow for transactions in official, government-backed fiat currency. Because virtual currencies can be exchanged and transferred peer-to-peer, users who use virtual currencies can limit their interaction with traditional, regulated financial institutions, which collect information about their customers and maintain anti-money laundering and fraud programs. WSM and its users were therefore able to bypass the traditional financial systems by only permitting virtual currencies as a means of payment.

g. WSM sellers (also known as vendors) were required to pay for their vendor account and provided a vendor webpage profile on WSM, akin to a storefront, where a vendor could advertise contraband. Vendors were given access to edit their webpage after logging into WSM. A vendor webpage included listings for contraband, and could include

pictures of contraband and instructions for users as to how to purchase such contraband and/or how it would be dispatched by the vendor.



h. Vendors on WSM received ratings from users, based on, among other things, the quality of contraband, reliability of delivery, and volume of traffic. In addition, WSM assessed rankings for vendors based on user input.

i. For each sale of contraband on WSM, WSM obtained a commission, ranging from approximately 2-5% of each transaction fee.

j. WSM provided security features for users and vendors. For example, WSM offered a platform for users to communicate with vendors with the option to encrypt their communications, such that only those parties involved could read the messaging between them.

k. For a customer to purchase contraband on WSM, based on having witnessed undercover purchases by case agents of contraband on WSM and my knowledge of this investigation, I am aware of the following:

- i. The customer selected contraband to purchase from a vendor and sent the vendor an order request.
- ii. The vendor acknowledged the customer's order request, agreed to sell the contraband to the customer.
- iii. The customer sent money to the vendor, generally through WSM (an escrow account hosted and created by WSM or a specified payment address WSM has created for the vendor).
- iv. Usually after the vendor confirmed on WSM that the contraband has been shipped, WSM released the funds to the vendor for payment from the customer, less commission fees retained by WSM.

11. Based on my training and experience, the creation, operation, and maintenance of websites, and specifically, darknet marketplace websites such as WSM, require individuals to conceptually design a website that functions properly and provides a seamless user experience, much like most e-commerce websites. Once conceptualized, the individuals have to write the computer code (in this instance, WSM was written in the programming language PHP) to design the website and all the functionalities for each feature offered (such as the ability to create vendor and buyer accounts, compile and associate user accounts and passwords, track and manage orders, confirm shipments, and dispense funds to all parties, offer private communications, etc.), and maintain the daily operation of the website on remote computer servers. In this case, the WSM administrators created, maintained, and operated WSM and were responsible for, among other things, ensuring that vendor pages functioned properly (e.g., vendors could post pictures of contraband to advertise their products), the overall website functioned properly, and that transactions for contraband were properly processed (e.g., users could pay for contraband, vendors could receive money, and the marketplace received its commission).

12. Several users of the site were hired by the administrators of WSM to work as "moderators." As described above, moderators are often employed by Darknet marketplaces to

resolve disputes between vendors and customers and to carry out other tasks. Before Reddit banned sub-reddits related to the Darknet, WSM hosted a sub-reddit (a topic page within the Reddit website). The WSM site had a hyperlink directing users to this sub-reddit. The sub-reddit listed all of the moderators of the sub-reddit, how long they had been moderating the sub-reddit, and what level of access they had to the sub-reddit.

13. As background, Reddit allowed for moderators to have differing levels of access to the sub-reddit. Moderators with “access” had authority to manage the lists of approved, banned, and muted users of the sub-reddit. Moderators with “flair” privileges could edit or control the text or icons displayed next to the poster’s username. Further, moderators with “mail” privileges were able to read and reply to moderator emails, and moderators with “posts” privileges were able to control the content of the sub-reddit’s messages.

14. I am aware that WSM has violated a number of U.S. federal laws. In the course of this investigation, federal law enforcement agents accessed WSM on numerous occasions and made undercover purchases, including of controlled substances, such as, methamphetamine and other drugs, in violation of 21 U.S.C. §§ 841 and 846; stolen credit card information and related tools, in violation of 18 U.S.C. § 1029(a) and (b); and counterfeit identity documents, in violation of 18 U.S.C. § 1028(a) and (f).

15. Undercover agents made these purchases by searching for goods on the WSM marketplace, clicking on links advertising the desired goods, and authorizing transfers of funds in connection with the transactions. Many of these purchases occurred from computers located in the Eastern District of California, as well as from law enforcement partners operating in the Central District of California. In addition, case agents have identified vendors on the site who were operating out of the Eastern District of California. I am also aware that some vendors of the site listed the sale of narcotics in Brazil.

B. Identification of Moderator “MED3L1N” and “MED3L1N WSM”

16. One of the primary moderators of the WSM sub-reddit was “MED3L1N_WSM.” This moderator account was opened in October of 2017, and had all of the above-described

privileges to the sub-reddit. In addition, as described below, on the WSM Forum, one of the primary moderators was “MED3L1N.” For the reasons described below, I believe that this Reddit account was operated by the same person operating the “MED3L1N” account on the WSM Forum. In addition, the information described below indicates that the person operating “MED3L1N” and “MED3L1N_WSM” is fluent in Portuguese and English.

17. On the WSM Forum, MED3L1N was listed as a “Community Manger.” MED3L1N was responsible for customer service, which included resolving disputes between vendors and customers on WSM. In addition, MED3L1N acted as a public relations representative for WSM, which included providing public responses to questions from customers. MED3L1N also provided advice to WSM customers, for example, by instructing them how to encrypt messages using PGP keys. This post and the ones described below were publicly available on the WSM and I have personally viewed them.

18. On February 20, 2018, MED3L1N created a post on the WSM Forum referencing “our official reddit r/WallStreet_Market/.” In that post, MED3L1N proposed that users of WSM leave reviews of vendors on the WSM site based on customer service, product quality, processing, price value, and operational security. At the end of the post, MED3L1N stated that this “template above would works [sic] only for drugs but we can create a template for fraud & related stuff too.”

19. On or about February 28, 2018, on the WSM sub-reddit, a user asked whether WSM was undergoing maintenance. Approximately one hour after this question was asked, MED3L1N_WSM responded by stating there was a post on the WSM Forum about the maintenance, and assured users that WSM would be back soon. Approximately one hour later MED3L1N_WSM informed the WSM sub-reddit that WSM was back online and everything was running fine.

20. In exchange for providing these services, MED3L1N was paid a salary by the administrators of WSM. In March 2019, I met with a European Law Enforcement (“ELE”) team regarding their investigation into WSM. ELE was able to obtain copies of the settings table of

the WSM servers, which contained notes regarding the website's development and payments for the administrators and moderators of the site. Contained in the settings tables was a note that "Med" was scheduled to be paid \$1,200, which I believe refers to MED3L1N and was his recurring salary payment for working on the site.

21. In March 2018, I obtained a search warrant for the contents of the MED3L1N_WSM account on Reddit. In response to the search warrant, Reddit provided me with the following items associated with the account: chat history, comment votes, comments, friend, IP logs, messages, post votes, posts, saved comments, saved posts, statistics, subscribed sub-reddits, and user preferences.

22. On January 30, 2018, MED3L1N_WSM created a post in Portuguese: "Opa sou moderador no WSM e gostaria de dar boas vindas (Apesar do topico ser antigo) ao /u/ bondedomaluco. Qualquer duvida ou problemas, so avisar, mandar mensagem, etc. Temos um forum e tambem o nosso sub :)." [Translation: Oops, I am a moderator on WSM and would like to welcome you (Although the topic is old) to /u/ bondedomaluco. Any questions or problems, just notify, send message, etc. We have a forum and also our sub :)]. This translation and all other translations referenced in this affidavit were made by me entering Portuguese text into Google Translate for the English translation. I also note that all posts/messages/writings referenced in this affidavit were made in English unless noted otherwise.

23. MED3L1N_WSM also made other comments in Portuguese, including on the same day, January 30, 2018. In one comment on that date, he/she stated "Sugior o Wall Street Market." In another comment on the same date, he/she stated "Como eu disse em um outro topico, compre btc e depois converta para xmr usando o shapeshift ou o changelly." [Translation: As I said in another topic, buy btc and then convert to xmr using shapeshift or changelly]. I know from my training and experience that "btc" is a common abbreviation for Bitcoin and "xmr" is a common abbreviation for Monero. I also know that Shapeshift and Changelly are online platforms that allow users to exchange one type of virtual currency for another.

24. On February 21, 2018, MED3L1N_WSM responded to a post on the WSM sub-reddit by “Xanaxcartel.” In the original post, Xanaxcartel complained about Xanax vendors on WSM defrauding customers and then leaving the WSM site. In response, MED3L1N_WSM stated that explained that “we” had raised the vendor bond to \$150, and that the operators of the site were attempting to balance the need to keep scammers away from the site with the competing interest of giving new vendors a chance to sell their products. As background, a vendor bond is an amount of money that vendors on WSM were required to put on deposit in order to list items for sale on WSM. I believe that this posting is sufficiently factual and specific to show that Reddit user MED3L1N_WSM was actually a moderator for WSM.

25. Further, on February 25, 2018, MED3L1N_WSM posted a comment in Portuguese: “Pessoal, em relacao aos servidores, pedimos sempre que usem outro mirror caso o primeiro estiver lento. Voce pode encontrar os mirros em nosso sub ou se o mod permitir posso postar aqui. Temos um total de 7 mirrors mais um mirror para TOR 3.0.” [Translation: Personnel, regarding the servers, always ask that they use another mirror if the first one is slow. You can find the mirrors in our sub or if the mod allows I can post here. We have a total of 7 mirrors plus a mirror for TOR 3.0]. As with the above posting, I believe that this posting is sufficiently factual and specific to show that Reddit user MED3L1N_WSM was actually a moderator for WSM.

26. On March 8, 2018, MED3L1N_WSM sent a private message on Reddit in Portuguese in which he/she discussed that he/she was leaving Reddit and moving to the Dread discussion forum. I know that around this time Reddit banned sub-reddits related to Darknet marketplaces, and that the persons identifying themselves as WSM sub-reddit moderators moved to the Dread Forum. MED3L1N_WSM continued to act as a moderator on the Dread Forum for WSM.

27. In their posts on Reddit and the WSM Forum, MED3L1N_WSM and MED3L1N frequently called people by the name “broder” in their posts and messages. I know from my training and experience that the term “broder” is slang for the term “brother.”

C. “MED3LIN” on Hansa Market

28. As background, in 2017, Hansa, behind AlphaBay, was estimated to be the world's second largest Darknet marketplace. In July of 2017, the Dutch National Police took over the operations of the Hansa Marketplace for a three-week period and were able to log information related to moderators, vendors, and users of the site. The takeover of Hansa Marketplace was coordinated with U.S. law enforcement's shuttering of AlphaBay, which took place on July 4, 2017. As a result of the takedown of AlphaBay, the moderators, vendors, and users of the site migrated to Hansa Marketplace, which, as described above, was being run by Dutch National Police for a three-week period. The migrating individuals were referred to as “AlphaBay refugees.”

29. As part of this migration, Hansa Marketplace user “MED3LIN” contacted the administrators of Hansa Marketplace on July 10 and 13, 2017 to request employment as a moderator with that site. These communications were logged by the Dutch National Police, who were actually running the site. The MED3LIN account was registered on July 7, 2017.

30. On July 10, 2017, MED3LIN wrote “Hello guys, I want to know, do you need anybody to help with disputes and/or support? I'm asking because once the number of users is growing so fast because of the new buyers and sellers coming from AB I think you will have to bring more people to help.” I know from my experience and training that “AB” is a commonly used abbreviation for AlphaBay. I also note that the spelling of this user's name has an “T” in the second to last letter instead of a “1” (which is how the name was spelled on Reddit and the WSM Forum).

31. In response to the inquiry from MED3LIN, the Dutch National Police asked him/her some follow up questions about his experience and background.

32. First, the Dutch National Police asked MED3LIN what skills or experience he/she had to offer. In response, MED3LIN stated “I have a large experience with support and moderation on bitcoin world. I already worked in a big p2p marketplace as moderator (Banning

scammers/rippers for instance) and support. I worked too in some small bitcoin exchanges in my country. On DNM I've always been around as buyer of tutorials, scripts, softwares.”

33. Second, the Dutch National Police asked which languages he/she spoke. In response, MED3LIN stated “English, Portuguese and a little of Spanish.”

34. Third, the Dutch National Police asked what levels of IT-knowledge he/she had, to which he/she replied “I'm a nerd. I have a little of knowledge in C# programming (I'm not programmer, just a curious). And I have knowledgement of network, servers (Building my own servers in many platforms), Linux (Since Debian until Raspbian for Raspberry PI). I have some courses but 90% of what I know I learned alone. I can say that I am a self taught person. Despite all these knowledgements, I don't think I will be useful on this area of the site. Hansa runs a amazing and big operation so you guys need the best of the best. I will be better helping in the support/moderation. Of course I know how to recognize a bug/problem and I will always report bugs, if I see anything wrong on the site or in the security, I can help giving tips, ideas, etc (I always did it on all my jobs).”

35. Fourth, the Dutch National Police asked what his/her availability would be, to which he/she replied “Anytime. I am workaholic so I am always up to help. I like to left my job without nothing pending. But a good time for me would be 12 PM - 11 PM London time (BST / GMT -1) and I can work everyday.”

36. Fifth, the Dutch National Police ask what he/she expected to get paid monthly by working on the Hansa site, to which he/she replied “It's really a hard question. I will give a price but you guys tell me if this is fair or not, I can help in any area of the site like forum, support and in Reddit for example. So USD 600 in BTC is a fair amount? If not, no problem.”

37. Sixth, the Dutch National Police asked what kind of off-site communications he/she used, to which he/she replied “I have jabber: med3lin@creep.im.” I know from my training and experience that the domain “creep.im” is a XMPP/Jabber server located in France. Jabber is an encrypted chat platform that allows individuals to communicate in a secure, anonymous manner.

38. Lastly, the Dutch National Police asked if anyone could vouch for him/her, to which he/she replied “Honestly I don't have anybody. I don't like to create relationship with anybody on dark web once I think this is not good for opsec. I have/had many others account here on Hansa and on Alphabay and also on Dream and Vahalla. I was always around buying fraud related stuff, reading the forum, etc. After use the account, I throw it away to avoid be "linked" with that account.”

39. Following the above-referenced communications, the Dutch National Police asked MED3LIN if he/she could provide them with a physical address to send a security token to in order to verify his identity. This was a ruse by the Dutch National Police to attempt to learn the real physical address of this user. MED3LIN responded with “I'm not sure if you were asking for my physical address or for an Email address. I don't think the physical address is safe to provide. As I said I live in SA, in anywhere in Brazil so the postal service is very slow and take a long time, sometimes 60 days and sometime we never receive the package.” He/she also provided an email address of med3lin@mail2tor.com. The statement by MED3LIN (on Hansa) that he/she lives in Brazil (where Portuguese is the spoken language) is consistent with MED3L1N_WSM's frequent postings and messages in Portuguese.

40. Even though MED3LIN stated that he/she did not want to provide a physical address, he/she eventually provided one to the Dutch National Police on July 17, 2019, in which he/she stated that his address was: Str: Joao Batista Pupo de Moraes, [Street Number Redacted by Affiant]; Neighborhood: Parque Industrial; City: Campinas; State: Sao Paulo; Country: Brazil; ZIP - 13031-690 (hereafter, the “Sao Paulo Address”). MED3LIN further stated that this was a drop address and that “Marcos Paulo is the guy who will receive then send to me.” I know from my training and experience that a drop address is a proxy address used by criminals to receive mailings. I know that drop addresses are often registered in a fake name or a name of a third-party who then sends the mailings to the true recipient. As described below, I believe that “Marcos Paulo” (full name **MARCOS PAULO DE OLIVEIRA-ANNIBALE**) is in fact the

real person behind the moniker MED3LIN, and that **ANNIBALE** stated that “Marcos Paulo” was the proxy recipient as an attempt to distance himself from the MED3LIN moniker.

41. MED3LIN further stated “Please, don't send the cops to this address or anything like this hahahahahaha just kidding. I know we are in dw but I trust you guys because Hansa support was always good and helpful so I don't think you will do any bad joke (This was my fear). I have this drop for a long time and I don't want to lost, if it's happen I will lost a lot of things.” I know from my training and experience that “DW” is often used as an abbreviation for Darkweb.

42. MED3LIN's last login to Hansa was on July 20, 2017, which is the date that U.S. and Dutch law enforcement first publicly announced the takedowns of AlphaBay and Hansa.

D. Investigation Into MARCOS PAULO DE OLIVEIRA-ANNIBALE

43. Upon learning of the address and name provided by MED3LIN to the Dutch National Police, I forwarded that information to the DEA's Sao Paulo office. My DEA colleagues in that office conducted a commercial database search for the Sao Paul Address, which revealed that it was associated with **MARCOS PAULO DE OLIVEIRA-ANNIBALE**, with a date of birth of March 26, 1990.

44. DEA Sao Paulo also obtained records of **ANNIBALE** from the Brazilian government, including his civil identification card, which listed a date of birth of March 26, 1990 and an address of the Sao Paul Address. The document also included the following photo of ANNIBALE as a child:



45. I also received records from the federal taxation agency of Brazil (Receita Federal do Brasil) for **ANNIBALE**, which listed a date of birth of March 26, 1990 and an address of the Sao Paulo Address. The records also list a company, Czar International Services, as being associated with **ANNIBALE**. The business's principal activity is listed as repair and maintenance of computers and peripheral equipment, its address is listed as the Sao Paulo Address, and the contact email address is "marcosannibale@gmail.com".

E. Online Profiles and Monikers Associated with ANNIBALE

46. I conducted multiple open source queries for the name **MARCOS PAULO DE OLIVEIRA-ANNIBALE**, which revealed several monikers and profile pages, including an eBay account under the username "marcosannibale1". Case agents issued an administrative subpoena to eBay in June of 2018 for records associated with this account. The results from that subpoena revealed that the account is registered to "Marcos Annibale," with an email address of "marcosannibale@gmail.com," the Sao Paulo Address, and a telephone number of 19989379254. The account was opened on March 4, 2016.

47. The eBay records for this account showed that **ANNIBALE** completed several purchases on eBay, including "Pure Copper Bitcoin Rounds Anonymous Mint Guardian Silk Road Coins." These Bitcoin Rounds are commemorative coins that have the Bitcoin symbol on it and also an image from the Silk Road Marketplace, which was the first Darknet marketplace. **ANNIBALE** also purchased a "3-Track Magnetic Card Reader," a "USB Laser Engraver Printer," a "Chip Blank Smart Card Contact IC Card," and an "MCR200 EMV Smart IC Chip Magnetic Stripe Card Reader and Writer." I know from my training and experience that these types of items are used for "carding," i.e. the use of credit cards and stolen identification information to steal funds or make fraudulent credit card purchases. The majority of IP addresses used to make these purchases on eBay are located in Sao Paulo, Brazil. All of the items were shipped to the Sao Paul Address.

48. For the “MCR200 EMV” card reader, the eBay records revealed that the purchase was completed on November 22, 2016, and that the product was shipped to the Sao Paulo Address. I conducted a search through the WSM Forum for “MCR200”, which returned several discussion threads. In those threads, MED3L1N commented on three threads offering advice on how to use the magnetic card reader. On December 27, 2017, MED3L1N stated on one of the threads, “I have one of this [sic], amazing machine.”

49. In conducting additional open source queries, I also found the website marcosannibale.me. The message “Hello World” is listed at the top of the website. The website listed a Bitcoin wallet address 1MArcoSBgoNhnypXD7YhE4T9B7eUFSTLA3. I note that the name “marcos” is included in this wallet address. A search of this address on the Bitcoin blockchain revealed that the wallet address had one transaction on or about December 13, 2017, in which it received approximately 0.0002628 Bitcoin. The website also listed a Monero wallet address. As noted above, the Monero is a virtual currency with an encrypted, private blockchain. I note that Bitcoin and Monero are the two types of virtual currencies accepted by WSM. The webpage also displayed a QR code and a public PGP key. I inputted the PGP key into a certificate manager, which provided the name "Marcos" and email address marcos@marcosannibale.com.

50. As background, Whois is a query and response protocol that is used to query databases storing the registered users or assignees of an Internet resource, such as a domain name or an IP address block. The Whois domain record for “marcosannibale.com” is registered to “Marcos Oliveira” at “Rua Paulo Pompeia Midas” in Sao Paulo with a phone number of +55.19989379254 and an email address of bit2youdotcom@gmail.com. I note that **ANNIBALE**’s full name is **MARCOS PAULO DE OLIVEIRA-ANNIBALE**, and that the listed phone number ending in 9254 is the same one that was listed on **ANNIBALE**’s eBay account.

51. Further, the historical Whois record updated on May 10, 2015 listed a registrant name of “Marcos Paulo De Oliveira Annibale,” a street address of “Joao Batista P de Moraes,” in Campinas, Sao Paulo, and an email address of “coinsofpixel@gmail.com.”

52. I also found a website associated with **ANNIBALE** at <https://about.me/marcosannibale>. The webpage listed the user’s name as “Marcos,” a “student, small business owner, and consultant in Campinas, Brasil.” The website also listed a PGP key of 0xbb70d6db67c25960, a website of <https://keybase.io/marcosannibale> and a TOR website of marcos5sttzmku4y.onion. I attempted to access both of the listed websites, but they were inactive. The website also listed links to an online profile on the website Github for user “CoinsOfPixel”, to the Twitter profile “DarknetCitzen”, and to “my website” at “marcosannibale.me”. A screen capture of this webpage is included below:



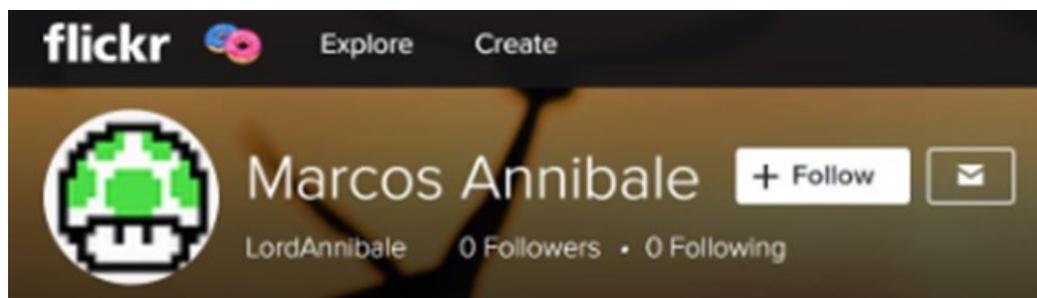
53. I also accessed the above-referenced “CoinsOfPixel” account, which stated “I am marcosannibale (<https://keybase.io/marcosannibale>) on keybase.” The listed website on Keybase was no longer active.

54. I also reviewed the Twitter account for user DarknetCitzen. The account was created in August of 2017 and listed its location as “Darknet.” On August 3, 2017, the user

posted a tweet stating “Hello World!” I note that the expression “Hello World” was also posted on the above-referenced website “marcosannibale.me.” Another tweet on January 18, 2018 stated “Verifying myself: I am marcosannibale on Keybase.io...” and provided a link to the above-referenced Keybase website.

55. I also found a Reddit post by user “darknetcitizen” under sub-Reddit KeybaseProofs. The post stated “I am: darknetcitizen on reddit, marcosannibale on keybase.” In that post, “darknetcitizen” was hyperlinked to Reddit user “Darknetcitizen’s” profile page, and “marcosannibale” was hyperlinked to the above-referenced Keybase website. Reddit user “Darknetcitizen” has no other listed posts or comments, and was registered on January 18, 2018.

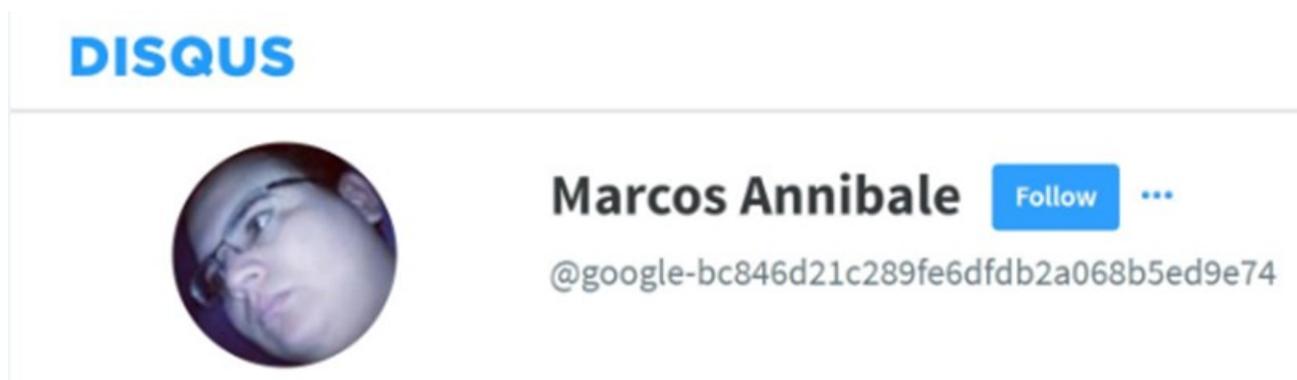
56. I also found a Flickr profile for “Marcos Annibale” that was created in May of 2011. On the “about” page was the image of a mushroom head that appeared to be the Mario Brothers video game, which is included below. This image was identical to the image on the above-referenced “about.me/marcosannibale” webpage. The about page for this Flickr account states in Portuguese “Sou nerd, gordo, megalomaniaco, viciado em games, ficcao, coisas tecnologicas, filmes de terror, comedia, interwebs (Amo isso). Ainda vou dominar o mundo” [translation: I’m a nerd, fat, megalomaniac, addicted to games, fiction, technological things, horror movies, comedy, interwebs. I will still dominate the world]. The Flickr page also listed the moniker “LordAnnibale.” I note that MED3LIN described himself as a “nerd” to the Hansa administrators.



57. I also identified a Facebook account for “DarknetCitizen”, which had an associated name of “Marcos Paulo”. The profile listed the above-referenced Bitcoin wallet

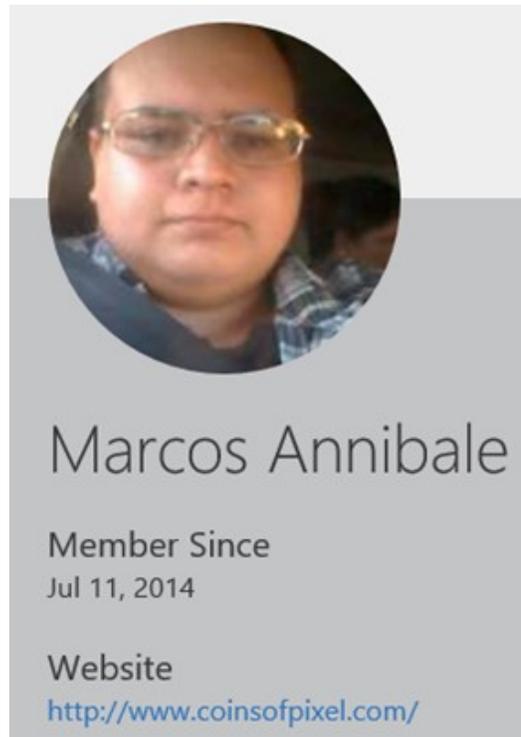
address of 1MarcoSBgoNhnypXD7YhE4T9B7eUFSTLA3. I noted that the listed Bitcoin wallet address was the same as the one listed on the website “marcosannibale.me.” The profile also stated that the user lives and is from Campinas, Sao Paulo, and joined Facebook in January 2015. The profile also listed the school Jose Maria Matosinho, which, according to online searches, is a state public school in Campinas, Sao Paulo, Brazil.

58. In addition, I identified a forum profile on the website “www.disqus.com” for user “Marcos Annibale.” The profile was created on November 9, 2012 and contains an image of a male wearing glasses, which is included below. A post on the profile references mining for Bitcoin in Brazil.



59. I further identified a forum post by “marcosannibale” on a Russian-based hacking forum located at <https://lolzteam.net/threads/73760>. The thread listed multiple email addresses and Steam (online gaming platform) account information with passwords. The thread listed an email address of marcosannibale@uol.com.br, a Steam username/password of “marcosannibale:campinas000,” and the game “Team Fortress 2.” As background, Team Fortress 2 is a team-based multiplayer video game. I note that “Campinas” is the municipality of the Sao Paulo Address. I further note that, as referenced above, ANNIBALE stated on his Flickr page that he is “addicted to games,” which I believe refers to video games, such as Team Fortress 2.

60. I also identified a social media page for ANNIBALE at <https://social.msdn.microsoft.com/Profile/marcos%20annibale>. As shown below, the page includes a photo of ANNIBALE and also references the website <http://www.coinsofpixel.com>.



61. The Whois domain record for “coinsofpixel.com” was listed for sale and had a historical Whois record updated on May 26, 2014 that listed the registrant as “Marcos Paulo De Oliveira Annibale” with a street address of “Joao Batista P de Moraes” in Campinas, Sao Paulo and an email address of coinsofpixel@gmail.com.

62. I also located a posting, dated September 20, 2016, on the web forum Bitcointalk.org, which linked to a news article about the founders of a large peer-to-peer Bitcoin exchange company Paxful. That posting also linked to the Paxful “About” page. A comment to the posting stated “So this is Marcos Annibale?” I then viewed the current Paxful “About” page and noted that it does not list anyone with the name of “Marcos.” However, I then searched for the Paxful webpage on the Internet Archive (a non-profit website the catalogues certain portions of the Internet), which revealed an older version of the Paxful website from late 2016 containing

a photo of an employee named “Marcos,” which I include below. Underneath the photo is a description of “Marcos” as the Customer Feedback Supervisor. As shown below, the photo was of a male with glasses in front of a bookcase. The individual in the photo appears to be the same person depicted in photos on the Microsoft and Disqus social media pages.



MARCOS

Customer Feedback Supervisor

Marcos makes sure the communication loop between users and developers is constantly improving.

63. I further noted that one of the books on the right side of the photo (over the left shoulder of **ANNIBALE**) is the book “Gomorra,” written by Roberto Saviano.



64. I then searched through the WSM Forum for any references to this book. I found that on May 28, 2018, MED3L1N posted a recommendation to read Roberto Saviano's book "Zero Zero Zero". In response, WSM vendor "AmmaccaBanane2" recommended the book "Gomorra". MED3L1N responded, "I read Gomorra, amazing book, the movie is cool too."

65. Pursuant to a subpoena, I obtained ANNIBALE's employment records from Paxful. The records confirm that ANNIBALE was an employee at Paxful. According to the records, ANNIBALE, on January 23, 2016, using email address marcosannibale@gmail.com, wrote an email to Paxful to request employment at Paxful as a customer service representative. ANNIBALE stated that he could help in the Portuguese and Spanish community, but if there was no need for support in these language, he could help the English speaking community as well. ANNIBALE introduced himself as "Marcos Paulo O. Annibale," a 25 year old Brazilian residing at the Sao Paulo Address. ANNIBALE's employment application also listed three telephone numbers including "(19) 9 8937-9254" and email addresses marcosannibale@gmail.com and cantatoannibale@gmail.com. I note that the above-referenced telephone number is the same one listed on ANNIBALE's eBay account.

66. The resume that ANNIBALE provided to Paxful listed his most recent work experience as being a computer and network technician from June 11, 2006 until "today." ANNIBALE also informed Paxful that his username on the Paxful site was "banqueiro" [Translation: banker]. The banqueiro account listed an email change on February 17, 2016, from futurobanqueiro@live.com to marcosannibale@gmail.com. I note that futuro banqueiro is Portuguese for "future banker."

67. I also conducted a query on the seized databases from AlphaBay, which revealed that user "banqueiro" purchased five key-loggers on January 14, 2016. Further, the password for the "banqueiro" account was "campinas000." I noted that Campinas is the municipality in Sao Paulo where ANNIBALE resides. Based on my training and experience, I know that key-loggers record keystrokes on a computer and are common tools of cyber-criminals to steal personal information such as passwords.

V. REQUEST FOR SEALING

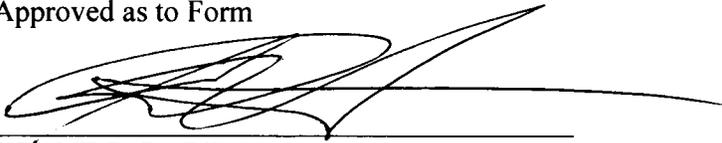
68. Because this investigation is continuing, disclosure of this affidavit and/or this application and the attachments thereto will jeopardize the progress of the investigation. The current investigation set forth above is not public, and I know, based on my training and experience, that criminals may attempt to destroy evidence if warned of the investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Accordingly, I request that the Court issue an order that this affidavit, application for a criminal complaint, and arrest warrant, be filed under seal until further order of this court.

[CONTINUED ON NEXT PAGE]

VI. CONCLUSION

69. Based on the foregoing, I believe that there is probable cause that **MARCOS PAULO DE OLIVEIRA-ANNIBALE** has committed violations of 21 U.S.C. §§ 841 and 846 (Distribution and Conspiracy to Distribute Controlled Substances) and 18 U.S.C. §§ 1956 and 1957. I therefore respectfully request that this Court issue a warrant authorizing agents to arrest **MARCOS PAULO DE OLIVEIRA-ANNIBALE**.

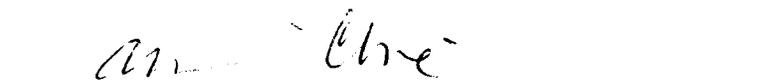
Approved as to Form



GRANT B. RABENN
RYAN WHITE
PUNEET KAKKAR
Assistant United States Attorneys
C. ALDEN PELKER
Trial Attorney


JAY D. DIAL, Jr., Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me on May 2, 2019.

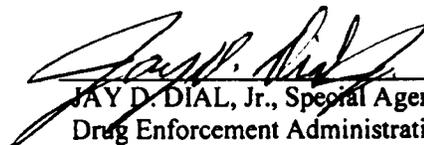

THE HONORABLE ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

VI. CONCLUSION

69. Based on the foregoing, I believe that there is probable cause that **MARCOS PAULO DE OLIVEIRA-ANNIBALE** has committed violations of 21 U.S.C. §§ 841 and 846 (Distribution and Conspiracy to Distribute Controlled Substances) and 18 U.S.C. §§ 1956 and 1957. I therefore respectfully request that this Court issue a warrant authorizing agents to arrest **MARCOS PAULO DE OLIVEIRA-ANNIBALE**.

Approved as to Form

GRANT B. RABENN
RYAN WHITE
PUNEET KAKKAR
Assistant United States Attorneys
C. ALDEN PELKER
Trial Attorney



JAY D. DIAL, Jr., Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me on May 2, 2019.



THE HONORABLE ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE