INDEX OF EXHIBITS

United States v. Thomas Mario Costanzo

CR-17-0585-01-PHX-GMS

EXHIBIT

A

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

1. I, Chad Martin, Task Force Officer of the United States Drug Enforcement Administration, Phoenix Field Division, Arizona, being duly sworn, hereby depose and state:

INTRODUCTION AND BACKGROUND OF AFFIANT

2. Your Affiant, Task Force Officer (TFO) Chad Martin, Scottsdale Police Department badge number 1294, has been employed by the Scottsdale Police Department since January 14, 2008, and was federally deputized as a Task Force Officer for the United States Drug Enforcement Administration (DEA), Phoenix Field Division (PFD) on July 2, 2015. Affiant Martin is currently assigned to the DEA PFD Task Force Group One (TFG1).

3. Your Affiant attended the Mesa, Arizona Law Enforcement Training Academy and received basic training in law enforcement practices and narcotics investigations. This training included the identification, investigation, and regulation of drug trafficking.

4. From June 2008, to April 2012, your Affiant worked as a patrol officer and participated in no fewer than one hundred arrests relating to illegal drugs. During that time, your Affiant became familiar with the ways in which illegal drugs are packaged and transported, as well as some of the common methods of operation used by drug traffickers to conceal and sell illicit drugs.

5. In May 2010, your Affiant attended the Scottsdale Police Department Narcotics Trained Officer (NTO) School. NTO School consists of advanced narcotics training, which covered the detailed identification, investigation, and regulation of drug trafficking including additional education in drug recognition and the techniques in which drugs are concealed, packaged, and transported.

6. In March 2011, your Affiant completed an Arizona Department of Public Safety course in marijuana and powder drug substance field testing. During this time, your Affiant became certified in the visual identification and chemical testing of marijuana,

methamphetamine, cocaine and cocaine base. Your Affiant was also trained in the classification and varieties of marijuana and the use, growth, packaging, and lifespan of marijuana.

7. In October 2011, your Affiant completed a 40-hour Scottsdale Police Department Drug Enforcement Unit Undercover School. During this school, your Affiant received advanced training in drug related surveillance operations, search and seizure procedures, the use and management of confidential informants, and undercover drug purchasing operations.

8. In April 2012, your Affiant was assigned to the Special Investigations Section of the Scottsdale Police Department, Drug Enforcement Unit. This Unit is responsible for investigating all aspects of drug related crimes in Scottsdale including narcotic, dangerous, and marijuana-related drug crimes, as well as local drug organizations responsible for the facilitation and distribution of illegal drugs and their related financial crimes. During this assignment, your Affiant investigated a multitude of drug related crimes including street level drug crimes, established drug trafficking organizations (DTOs), prescription fraud organizations, money laundering, and asset forfeiture investigations. Since April 2012, your Affiant has operated as both the Case Detective and Undercover Detective on a multitude of investigations, including numerous hand-to-hand drug transactions, and has received first-hand knowledge of how street drugs are packaged, concealed, transported, sold, and used. Your Affiant has debriefed and managed multiple confidential informants and has gained experience managing confidential informants during covert drug operation.

9. In July 2012, 2013, and 2014, your Affiant attended the Arizona Narcotics Officers Association (ANOA) Conference. During these conferences, your Affiant attended numerous seminars related to drug investigations and received advanced training on drug cartels, common drug trafficking methods of criminal

motorcycle gangs, and training on the methods and practices of drug trafficking organizations (DTOs).

10. In May 2013, your Affiant attended a one-week International Narcotics Interdiction Association (INIA) interdiction seminar. This training provided your Affiant focused information on interstate drug trafficking, including methods commonly used by drug traffickers to covertly transport drugs and currency across state lines and avoid detection by law enforcement.

11. In May 2015, your Affiant was assigned to the United States Drug Enforcement Administration (DEA), Phoenix Divisional Office, as a Task Force Officer (TFO) and was federally deputized on July 2, 2015. By virtue of my employment as a Task Force Officer, your Affiant has performed various tasks, which include, but are not limited to:

a) Functioning as a surveillance agent, thus observing and recording movements of persons trafficking in drugs and those suspected of trafficking in drugs;

b) Interviewing witnesses, confidential sources (CS) and sources of information (SOI) relative to the illegal trafficking of drugs and the distribution of monies and assets derived from the illegal trafficking of drugs (laundering of monetary instruments);

c) Functioning as a case agent, entailing the supervision of specific investigations involving the trafficking of drugs and the laundering of monetary instruments;

d) Initiating and monitoring of Title III investigations; and,

e) Conducting complex financial investigation involving the structuring, placement, and layering of large amounts of U.S. currency.

12. In the course of conducting drug investigations, you Affiant has personally interviewed informants and persons involved in the distribution of illegal drugs. These persons include users of illegal drugs, sellers of illegal drugs, and experienced federal, state, and local drug enforcement officers. Your Affiant has consulted with other experienced investigators concerning the practices of drug traffickers and the best methods of investigating them. Your Affiant is familiar with the methods used by those engaged in illegal drug and controlled substance activities to conduct their business, transport and distribute their products, protect their associates, conceal their identities, avoid detection and identification of their assets, activities, and whereabouts. All of these sources of information have provided your Affiant with objective details about the methods and practices of drug crime investigations.

13. Your Affiant has aided in no fewer than five wiretap investigations. Your Affiant has conducted physical surveillance, acted as a line investigator, line supervisor, conducted follow up investigation, and participated in arrests, the execution of search warrants, and interviews of subjects related to wiretap investigations.

14. In preparing this Affidavit, your Affiant has conferred with other experienced detectives and law enforcement officers who share the opinions and conclusions stated herein. Furthermore, your Affiant has personal knowledge of the facts discussed in this Affidavit, or learned them from the individuals mentioned herein.

15. Your Affiant also relies on his experience, training, and background as a Task Force Officer with the DEA in evaluating this information.

16. Throughout the course of this investigation, your Affiant has extensively researched crypto-currency technology. Your Affiant has learned the ways in which Bitcoin and other digital currencies known as Altcoins are utilized as both a store of value and as a method of payment in a digital environment. Your Affiant has learned that these peer-to-peer decentralized crypto-currencies utilize publicly distributed blockchain technology to facilitate the movement of funds throughout the world. Because of this technology, your Affiant knows that money can be

easily laundered and sent anywhere in the world using Bitcoin. Your Affiant has attended multiple meetings related to virtual currency and conferred with experts in the field of Bitcoin and blockchain technology.

RELEVANT CRIMINAL STATUTES AND PURPOSE OF AFFIDAVIT

17. On the basis of the facts herein, your Affiant submits there is probable cause to believe that violations of Title 18 U.S.C. §§ 371 and 1960(a) (Conspiracy to operate unlicensed money transmitting business), 18 U.S.C. §§1960(a) and 1960(b)(1)(B) (Operation of unlicensed money transmitting business), 18 U.S.C. 1956(a)(3)(B) (Money laundering to conceal or disguise the nature, location, source, or ownership of proceeds represented by a law enforcement officer to be proceeds of drug trafficking in violation of 21 U.S.C. §§ 841 and 846), and 18 U.S.C. 1956(a)(3)(C) (Money laundering to avoid transaction reporting requirements of proceeds represented by a law enforcement officer to be proceeds of drug trafficking in violation of 21 U.S.C. §§ 841 and 846) have and/or will be committed by subjects described within this Affidavit. Your Affiant requests a warrant to search and seize evidence from the following properties and vehicle which are being utilized to facilitate the crimes described above.

18. The target properties and vehicles requesting to be searched are as follows:

a) AN APARTMENT UNIT located at [redacted] further described in attachment A-1. This is a multi-unit, two story apartment complex located on the northeast corner of the intersection of [redacted] Specifically, Unit [redacted] is located on the second story, far south end of the complex. Unit [redacted] is the first unit located at the top of the most southern staircase. The front door to the unit faces west and has a tan in color metal security door. At the time of this writing, there is a piece of white paper in the front window to the unit with the numbers [redacted]" printed in black.

b) A RESIDENCE located at [redacted] as further described in attachment A-2 This is a single story residence with a tan brick exterior and a brown shingle roof. [redacted] Peter STEINMETZ as the owner of the property. (Further identified in attachment A-2)

c) The VEHICLE identified as a 2000 **Porsche Boxster**, red in color, displaying Arizona license plate "SATOSHI", assigned VIN: [redacted] currently registered to Peter STEINMETZ at [redacted] hereinafter referred to as "**Porsche Boxster**"), as described in attachment A-3.

19. Pursuant to Title 18 U.S.C. § 982 (Criminal forfeiture), incorporating the procedures governing forfeitures for violations of Title 18 U.S.C. §§1956(a)(3)(B), 1956(a)(3)(C), 1960(a), and 371, your Affiant further submits that there is probable cause for the seizure and forfeiture of the following vehicle:

a) The **Porsche Boxster** referred to as above, which is specifically identified as a 2000 **Porsche Boxster**, red-in-color, displaying Arizona license plate "SATOSHI", assigned VIN: [redacted] currently registered to Peter STEINMETZ at [redacted] (hereinafter referred to as "**Porsche Boxster**"), as described in attachment A-3.

BACKGROUND ON BITCOIN

20. Bitcoin is a digital, non-regulated, crypto-currency which operates independently of a central bank or single administrator and is held electronically, commonly on a computer, cellphone or tablet. It is a peer-to-peer system and transactions take place between users directly, without an intermediary. Because there is no central

oversight or authority, Bitcoin transactions are verified by network nodes and recorded in a public ledger called the blockchain.

21. Bitcoin is pseudonymous, meaning that the digital currency is not tied to an identifiable real-world entity but rather to a Bitcoin address. Owners of a Bitcoin address are not explicitly identified and new addresses can be generated for every new transaction to increase anonymity. A digital or paper wallet stores the information necessary to facilitate a Bitcoin transaction and contains an individual's Bitcoin holdings.

22. The purchase and sale of Bitcoin can be conducted either through an online website exchange such as Coinbase.com, or through an in person peer-to-peer transaction that does not use an established exchanging service as an intermediary. Peer-to-peer transactions can be conducted by individuals meeting in person where the seller sends Bitcoin from their digital Bitcoin wallet directly to buyer's Bitcoin wallet in exchange for a predetermined amount of fiat currency.

23. The Financial Crimes Enforcement Network (FinCEN) has specific guidelines and regulations pertaining to persons who administer or exchange virtual currencies such as Bitcoin. These regulations define a person who is an administrator or exchanger of virtual currency as someone who accepts real currency or its equivalent from a purchaser, and transmits the value of that currency into virtual currency. This activity is classified as a money transmission business and requires a person acting as a Bitcoin exchanger to be registered as a Money Service Business (MSB) with the United States Secretary of the Treasury.

24. A lawful Bitcoin exchange should adhere to federal anti-money laundering laws (AML) and Know Your Customer (KYC) guidelines to ensure they are following FinCEN guidelines and not breaking any United States money laundering laws. The objectives of AML and KYC is to prevent MSB's from being used for money laundering activities and allow MSB's to better understand their customers and their financial dealings. There are several legitimate Bitcoin exchanges operating in the United States that follow FinCEN regulations and charge fees as little as 1.5

percent for their services to convert fiat currency into Bitcoin.

25. Your Affiant has learned that there are peer-to-peer Bitcoin transactions conducted with non-registered exchangers typically to avoid reporting requirements under State or Federal law. These non-registered Bitcoin exchangers tend to meet with Bitcoin purchasers in person and typically charge a much higher fee of up to 10 percent for their services. Your Affiant knows based on training and experience that individuals who purchase Bitcoin from non-registered exchangers are willing to pay a higher fee to avoid the filing of a currency reporting form so that their identity and the transaction can remain anonymous, and the origin of the funds is untraceable.

26. Throughout this investigation, investigators identified a publically accessible website called Localbitcoins.com that facilitates the purchase and sale of Bitcoin by allowing exchangers to list their services and contact information on their website so that customers interested in exchanging U.S. Currency for Bitcoin may contact them. Typically, the customer contacts the Bitcoin exchanger who appealed to their interest. They communicate and if they reach an agreement, they ultimately arrange an in-person meeting where they conduct a peer-to-peer Bitcoin exchange/transaction. The transaction consists of the customer handing a predetermined amount of U.S. Currency to the exchanger, who upon receipt of the currency, electronically transfers the negotiated amount of Bitcoin to the customer's electronic wallet. Localbitcoins.com allows people to create anonymous profiles because they only require users to provide an email address. As a result, many of the Bitcoin exchangers who advertise their services on localbitcoins.com provide an alias or fictitious moniker for their user name and are not registered with the U.S. Secretary of the Treasury.

PROBABLE CAUSE

CASE BACKGROUND AND INITIAL IRS INVESTIGATION

27. In March, 2015, Agents from the Internal Revenue Service (IRS) began

investigating localbitcoins.com and identified the Bitcoin exchange profile of "Morpheus Titania," who was the top rated cash Bitcoin exchanger in Phoenix, Arizona. Morpheus Titania advertised the sale of Bitcoin in exchange for cash throughout the Phoenix Metropolitan area and lists his phone number as (602) 434-1725 on the localbitcoins.com website. He states the following in the "Terms of trade" section of his profile:

> *Contact hours: I am up late so TEXT me anytime. TEXT me for best and fastest response. I will get you Bitcoins immediately and discretely!*
>
> *Meeting preferences: Mcdonalds, Starbucks, Paradise Bakery.*
>
> *I have the fastest response times. I travel all over town so u can get the Bitcoins u want and need NOW! TEXT me six-oh-2-four-3-four-one-seven-two-five for fastest and best response.*
>
> *All transactions are done complete anonymity. The only only record of the transaction is on the blockchain.*
>
> *I am on time, every time. You will see why I have more trades than anyone else around! I love to talk about how Bitcoin is changing the world. I know it has been the best thing I have ever done, IN MY ENTIRE LIFE.*
>
> *I can teach u about not getting scammed too. I got scammed by Indian Scammer guy named "William" love to tell you a story about him! BeWARE of anyone wanting to transfer funds to u via Paypal or Venmo. I am available for consultation whether you buy from me or not!*
>
> *I love working with both newbie's and pros! Hit me up and u will see why my customers come back to me again and again. I tell u straight how it is.*
>
> *I am very friendly and I love to talk. Text me so I know that you want to meet. My customers let you know its worth it to deal with me. :)*
>
> *Lately I also trade on mycelium App under Morpheus Titania.*
>
> *http://www.titanians.org/who-is-morpheus/*
>
> *Have a great Day looking forward to connecting!*

28. The localbitcoins.com profile for Morpheus Titania shows the profile was created on March 12, 2013, and had "100+" confirmed transactions with a 100% feedback score. The profile shows that Morpheus Titania charges different prices for Bitcoin sales depending on what city traveled to and the amount of Bitcoin being purchased. Morpheus Titania's fees typically range from a price of 7 percent to 10 percent above the average market price per Bitcoin. The profile advertises that Morpheus Titania can sell between $200 - $30,000 worth of Bitcoin during a single transaction.

29. Investigators later identified Morpheus Titania as a male named Thomas COSTANZO (hereinafter referred to as "COSTANZO"). This identification was based upon subpoenaed information received from T-Mobile USA / MetroPCS for the (602) 434-1725 telephone number provided by Morpheus Titania on localbitcoins.com. Investigators learned that (602) 434-1725 is subscribed to Thomas COSTANZO, and lists a customer name of "Morpheus Titania." The identification was also confirmed from multiple undercover meetings with COSTANZO where he identified himself as "Morpheus" and was confirmed by investigators to be Thomas COSTANZO via Arizona Motor Vehicle Department (MVD) photographs.

30. On March 21, 2015, an Undercover Agent (UCA1) from the Internal Revenue Service (IRS) attended a Bitcoin meet up event in Phoenix, Arizona that was advertised on the internet and is typically held once a month to facilitate the meeting of people involved in Bitcoin technology and the use of digital currencies. UCA1 had previously contacted COSTANZO through the localbitcoins.com website regarding the purchase of Bitcoin and was invited to the meeting by COSTANZO the day before.

31. During the meeting, it was learned that COSTANZO is a co-organizer of the event. UCA1 sat at a table with a few other individuals who were attending the meeting. One of the individuals introduced himself as "Peter" and was later identified as Peter STEINMETZ (hereinafter referred to as "STEINMETZ") based

on his Arizona MVD photograph and a photograph that was posted on http://STEINMETZ.org/peter. STEINMETZ claimed to be a "wholesaler" of Bitcoin during the meeting and explained how he had been conducting Bitcoin transactions with COSTANZO since 2013. STEINMETZ went on to explain that while COSTANZO would meet with just about anyone to do a Bitcoin transaction, he prefers to meet with fewer people and do large transactions. STEINMETZ claimed to be in the business of trading Bitcoin since 2010 and stated that he does a lot of international buying and selling of Bitcoin. STEINMETZ advised that he primarily got into Bitcoin for political reasons and told UCA1 that he likes that Bitcoin is a currency the government can't manipulate. STEINMETZ spoke to UCA1 about Suspicious Activity Reports and how he believes several of those reports have been filed on him due to his large transactions. STEINMETZ also spoke about structuring cash deposits at banks by breaking the large deposits up into smaller amounts. STEINMETZ advised that he uses computer software to keep track of his Bitcoin transactions and trading accounts. He explained that a program called "GNU Cash" is one of the programs he uses. STEINMETZ made it known to UCA1 that he does, and is able to do very large cash to Bitcoin transactions, charging a 5 percent fee to exchange Bitcoin. He explained that he does many thousands of dollars in volume. STEINMETZ and COSTANZO spoke to UCA1 at length about Bitcoin and revealed that they met each other on localbitcoins.com. STEINMETZ also stated that he has worked with COSTANZO for some time exchanging Bitcoin.

32. On May 20, 2015, UCA1 met with COSTANZO to exchange $3,000 of cash for Bitcoin. During the meeting, the UCA1 began by informing COSTANZO that he needs the Bitcoin to pay his supplier for heroin. UCA1 informed COSTANZO that he buys black tar heroin in Arizona from his supplier for $27,000 a kilo and ships the heroin to New York to sell it for $50,000 a kilo. UCA1 told COSTANZO he needs to exchange between $15,000 - $30,000 at a time and asked COSTANZO if he was able to fulfill that. COSTANZO responded with "Yeah,

whatever you want." COSTANZO claimed to have done "about half a million in the last year."

33. UCA1 explained to COSTANZO that he pays his suppliers in Bitcoin to which COSTANZO responded, "Yeah, that is so much easier. Bitcoin makes everything so much easier." They concluded the meeting and successfully exchanged $3,000 U.S. currency into Bitcoin.

34. On October 7, 2015, another IRS Undercover Agent (UCA2) met with COSTANZO at a restaurant in Phoenix, Arizona to conduct a Bitcoin exchange. During the transaction, UCA2 was acting as a partner of UCA1 and stated he was meeting COSTANZO to conduct the Bitcoin purchase related to their business. UCA2 originally set up the meeting telling COSTANZO he wanted to exchange $10,000 cash for Bitcoin. When the meeting took place, UCA2 told COSTANZO he actually had $15,000 in U.S. Currency and would like to exchange all of it for Bitcoin. COSTANZO told UCA2 that he only had enough Bitcoin on him to exchange $13,000, but agreed to meet later that day to exchange the rest. During the meeting, COSTANZO told UCA2 that he was planning to start using a Bitcoin storage device called a "Trezor." Your Affiant knows that a Trezor is an electronic digital currency storage device, similar to a USB memory stick, which contains and encrypts cryptographic private keys used to store digital currency assets such as Bitcoin. COSTANZO then completed the exchange of $13,000 for Bitcoin with UCA2.

35. After the Bitcoin exchange was complete, a surveillance team followed COSTANZO as he left the meeting location. COSTANZO drove directly to [redacted] address for STEINMETZ. COSTANZO remained at the [redacted] for approximately 10 to 15 minutes. Your Affiant believes that COSTANZO traveled to the [redacted] so that STEINMETZ could resupply COSTANZO's Bitcoin account since COSTANZO sold $3,000 more Bitcoin to UCA2 than COSTANZO

had originally planned. Your Affiant believes COSTANZO needed more Bitcoin to conduct his prearranged sales for the day and maintain his 100% positive feedback on localbitcoins.com. Based on this and the previous communication between STEINMETZ, COSTANZO and UCA1, your Affiant believes that STEINMETZ is a Bitcoin supplier for COSTANZO and has access to large amounts of Bitcoin.

36. As COSTANZO departed the [redacted] surveillance units followed COSTANZO to two public locations and observed him conduct a Bitcoin transaction at each location. Investigators were unable to identify the individuals COSTANZO met with at each location.

37. On November 21, 2015, UCA1 contacted COSTANZO about doing another Bitcoin exchange. COSTANZO invited UCA1 to a Bitcoin meet-up group event being held at a public venue in Phoenix, Arizona. UCA1 attend the event and observed STEINMETZ was present at the meeting and was conducting a trade with another person. After STEINMETZ completed the exchange with the person, UCA1 then gave $2,000 U.S Currency to STEINMETZ in exchange for Bitcoin. STEINMETZ indicated to UCA1 that he would have more Bitcoin available in the future and provided UCA1 with a business card advising that he could call him to discuss a larger transaction. During this same meeting, UCA1 also met with COSTANZO and exchanged $13,000 worth of U.S. currency for Bitcoin.

38. Investigators conducted a blockchain analysis of the Bitcoin transfer from STEINMETZ to UCA1 and learned that STEINMETZ used a wallet from a Bitcoin exchange located outside of the United States (hereinafter referred to as "BCE1") to transfer $2,000 worth of Bitcoin to into UCA1's wallet.

39. Pursuant to a subpoena, investigators learned that in March 2013, STEINMETZ opened an account with BCE1. Investigators learned that BCE1 allows trading between U.S. currency and Bitcoin usually for a fee of 1 to 2 percent. BCE1 also allows U.S. currency and Bitcoin deposits and withdrawals. BCE1 records indicated that over an approximate two-year period, STEINMETZ traded

approximately one million dollars' worth of U.S. currency. Investigators also learned that in December 2013, BCE1 asked STEINMETZ a series of Know Your Customer (KYC) questions in order to increase withdrawal thresholds for STEINMETZ. STEINMETZ responded to the KYC questions informing BCE1 that he uses funds to trade between exchanges and listed three banks he was using to withdraw funds. STEINMETZ listed First Bank as one of the three financial institutions where he held an account for the purpose of transferring funds from his BCE1 account. Based on this information and the transfer of Bitcoin to UCA1 from STEINMETZ' BCE1 wallet, your Affiant believes that STEINMETZ holds an account with BCE1 to engage in the unlawful exchange of currency in the United States.

40. On Feb 29, 2016, UCA1 called STEINMETZ to discuss meeting with him again to exchange cash for Bitcoin and discuss future business together. UCA1 asked STEINMETZ if he could exchange $22,000 to $23,000. STEINMETZ advised that he could do that and it was definitely over his minimum transaction amount. STEINMETZ informed UCA1 that his fee would be 5 percent and that with "those volumes of cash" STEINMETZ wanted to meet at his house where he uses a cash counter. STEINMETZ told UCA1 that his address is [redacted] They arranged the meeting for March 8, 2016. STEINMETZ informed UCA1 that his wife does not like him doing business inside the house, so he does it in the garage.

41. On March 8, 2016, UCA1 met STEINMETZ at the [redacted] where STEINMETZ took UCA1 into his garage to conduct the Bitcoin exchange. Prior to the exchange, UCA1 stated that the cash he brought was from the sale of drugs. STEINMETZ then refused to conduct the transaction with UCA1 explaining he could not complete the transaction because he was now aware the cash was from drug proceeds and would be considered money laundering under federal laws. STEINMETZ told UCA1 that there was a Bitcoin meet-up event that night where someone might be there to conduct the transaction with him.

CURRENT INVESTIGATION

42. Since March 2016, your Affiant, along with other members of the Drug Enforcement Administration (DEA) Task Force Group One (TFG1), members of the United States Postal Inspectors Service (USPIS), the Internal Revenue Service (IRS), and the Department of Homeland Security (DHS) have been conducting a Joint Task Force investigating the money laundering and drug trafficking activities of multiple individuals utilizing a hidden portion of the internet known as the Darknet to facilitate the sale, transportation, and distribution of illegal drugs throughout the United States in exchange for the digital crypto-currency Bitcoin. Because transactions on the Darknet are conducted with digital crypto-currency, investigators have identified Bitcoin exchangers in the Phoenix area who are unlawfully exchanging Bitcoin for U.S. Currency with individuals frequenting the Darknet for illicit activities. Because of the identification of Bitcoin exchangers, the Joint Task Force expanded their investigation to incorporate the money laundering and unlicensed money transmission business activities being conducted by Bitcoin exchangers, including COSTANZO and STEINMETZ.

43. Open source and law enforcement data base queries were conducted on COSTANZO and STEINMETZ to inquire if either has a lawful money transmission business for the purpose of exchanging of U.S. Currency for Bitcoin. Investigators found that while COSTANZO has multiple Bitcoin related videos, interviews, and podcasts posted on the internet explaining Bitcoin technology, COSTANZO does not have any money transmission business documentation filed with FinCEN or with the Arizona Department of Financial Institutions ("AZDFI") that would authorize him to operate a money transmission business and exchange Bitcoin for other forms of currency. In regards to STEINMETZ, investigators learned that the Arizona Corporation Commission lists him as the Statutory Agent of BITCOINANDMORE, LLC, registered in the name of Peter STEINMETZ with an address at the [redacted] A FinCEN and AZDFI query of STEINMETZ and the BITCOINANDMORE, LLC was conducted revealing that

neither name was registered as a licensed money transmission business.

44. In September, 2016, your Affiant, acting in an undercover capacity, reviewed the localbitcoins.com profile being operated by COSTANZO, and then contacted COSTANZO on multiple occasions to conduct cash Bitcoin transactions. These transactions are described in detail below:

45. On September 14, 2016, your Affiant, acting in an undercover capacity contacted COSTANZO via a text message at the telephone number COSTANZO advertises on localbitcoins.com (602-434-1725) to initiate the purchase of Bitcoin. Your Affiant arranged a meeting with COSTANZO for that same day at a restaurant in Mesa, Arizona, to purchase approximately 3 Bitcoins in exchange for $2,000 in U.S. Currency.

46. Later that day, your Affiant met with COSTANZO (identified via MVD photographs as Thomas Mario COSTANZO) at the previously agreed upon meeting location. COSTANZO approached your Affiant and introduced himself as "Morpheus" (his alias from localbitcoins.com). COSTANZO and your Affiant made small talk for approximately twenty minutes where COSTANZO explained his anti-government, anti-banking, anti-establishment views to your Affiant. COSTANZO relayed that he believes the banking system is corrupt and only serves as a means for the government to control its citizens. COSTANZO explained in detail how Bitcoin works and how peer-to-peer cash Bitcoin transactions are conducted to avoid the need for any banking institutions or government regulations. COSTANZO informed your Affiant that he knows "a guy" who can get him $100,000 in Bitcoin and advised that he has done approximately a quarter million dollars in transactions with that person (all unreported to the U.S. government). COSTANZO stated that for large transactions like that, "his guy" purchases Bitcoin off a Bitcoin exchange linked to a bank account. That person then sells the Bitcoin to COSTANZO at a slightly higher price than he paid, and COSTANZO sells the Bitcoin to his customer at a slightly higher price so they both make money. Based on the prior IRS

undercover meetings with COSTANZO and STEINMETZ, your Affiant believes that the "guy" COSTANZO was referring to is STEINMETZ.

47. Your Affiant believes based on training and experience that because COSTANZO charges a fee of up to 10 percent above the average market price per Bitcoin, it is unlikely people would conduct business with him if their funds came from a legitimate source. Your Affiant further believes that COSTANZO is aware he is laundering proceeds from illegal activity with Bitcoin by charging such a high exchange price and not following any AML or KYC protocols. This is also based on statements COSTANZO made to your Affiant about his anti-government beliefs and his admissions that Bitcoins allows people to conduct transactions anonymously without any government regulations.

48. COSTANZO expressed that there are no limits to Bitcoin and that if we wanted to conduct a 10-million-dollar transaction, we could do it. COSTANZO advised that he has no business costs because he utilizes public places for free to conduct his Bitcoin transactions and keeps all of his Bitcoin storages on his cell phone or his electronic Bitcoin storage "Trezor" device. As previously learned during this investigation, your Affiant was aware that a Trezor is an electronic digital currency storage device, similar to a USB memory stick which contains and encrypts cryptographic private keys used to store digital currency assets such as Bitcoin.

49. Your Affiant asked COSTANZO about the security of Bitcoin and whether the government can track transactions. COSTANZO advised that Bitcoin is pseudonymous and that there are ways to make it difficult to track. COSTANZO also advised that localbitcoins.com is a good way to conceal money transactions.

50. Your Affiant spoke to COSTANZO about the his use of the Darknet and told COSTANZO that he was looking to purchase items on the Darknet and use Bitcoin as payment method because it is secure. COSTANZO advised that the issue with trusting sites on the Darknet is that the websites can be taken down.

51. Your Affiant advised COSTANZO that he has a need to transport large quantities

of money between Arizona and California and was trying to avoid having the money seized if stopped by law enforcement. COSTANZO stated that this is why Bitcoin is so useful and that there are no limits, especially if you want to transport currency internationally. Your Affiant told COSTANZO that he would like to purchase around $30,000 in Bitcoin on a regular basis. COSTANZO stated, "if you are doing anything illegal, I don't want to know about it". COSTANZO advised that his business model is, "I don't care who you are, what you are, where you are," that he only cares that "you don't get bit, don't get shot, and don't talk to any police". COSTANZO then informed your Affiant about a previous customer he had who wanted to send money and "stuff in car parts to Russia". Your Affiant believes COSTANZO was referring to the drugs conversation he previously had with UCA1. COSTANZO stated that was the kind of stuff he does not need to know, that it does not make any difference to him, and that it is none of his business. Your Affiant then purchased $2,000 worth of Bitcoin from COSTANZO. During the purchase of Bitcoin, COSTANZO charged a 10 percent fee for the exchange service.

52. Your Affiant conducted research of COSTANZO and learned that COSTANZO lists [redacted] as his residential address on his Arizona Motor Vehicle Department (MVD) record.

53. On November 16, 2016, your Affiant, acting in a UC capacity, contacted COSTANZO at his advertised telephone number and initiated a second Bitcoin purchase from COSTANZO in the amount of $12,000 U.S. Currency. Your Affiant met with COSTANZO on that same date at public venue in Tempe, Arizona, where COSTANZO again started the conversation by explaining his anti-government beliefs. Your Affiant told COSTANZO that he is purchasing the Bitcoin to transport currency across the country without having to worry about law enforcement seizing the money. COSTANZO agreed that Bitcoin is great for that and explained that he has a guy who once exchanged $60,000 with him.

COSTANZO stated that the guy had to go around to several different banks and withdraw a few thousand dollars at a time to avoid getting a suspicious activity report (SAR) generated on him. COSTANZO explained to your Affiant that anytime someone withdrawals more than $3,000 at a time, the bank will complete a SAR for the government to document the transaction. These statements lead your Affiant to believe that COSTANZO is aware of United States money laundering laws and currency reporting regulations and is knowingly using Bitcoin to circumvent the law and launder proceeds from illegal activity.

54. During the conversation, COSTANZO said "you can do whatever you want, you can do something illegal, I don't want to know about it." COSTANZO again advised that he only cares about three things, "don't get bit, don't get shot, and don't talk to any police". COSTANZO then sold your Affiant $12,000 worth of Bitcoin including his money exchange fee of 7 percent for the exchange. While the exchange was taking place, COSTANZO told your Affiant about another customer of his who regularly exchanges approximately $600 for Bitcoin every week. COSTANZO complained of how that particular customer sometimes pays him in several $1 bills. COSTANZO stated this is because the customer gets the cash from "his girls" because he is a "pimp".

55. After the transaction between your Affiant and COSTANZO was complete, surveillance units followed COSTANZO as he got on his bicycle and rode away from the deal location. Surveillance units followed COSTANZO to a light-rail train station where he took the light-rail to Phoenix. Investigators followed COSTANZO and watched him meet with several other people conducting what appeared to be cash Bitcoin transactions. Investigators then followed COSTANZO as returned to the light-rail and took a train back to the area of E. Main Street / N. Center Street in Mesa. Surveillance was concluded as COSTANZO appeared to be returning to the [redacted]

56. Based on subpoenaed information received from T-Mobile USA / MetroPCS, your Affiant learned that the telephone number utilized by COSTANZO has a

subscriber of Thomas COSTANZO, listing a customer name of "Morpheus Titania" at an address of [redacted] Your Affiant researched the [redacted] address and learned that it is the address of the "Brown Road Marketplace," a public shopping complex located in Mesa. Your Affiant believes that COSTANZO is attempting to conceal his identity and residential address by listing a public place as his cell phone billing address.

57. On December 1, 2016, the Honorable Michelle H. Burns, United States Magistrate Judge signed Order 16-543MB authorizing the release of location information and the use of signal tracking technology on COSTANZO's cellular telephone 602-434-1725 between December 1, 2016 and January 14, 2017. Your Affiant obtained and reviewed the location tracking information for the telephone between December 5, 2016 and December 12, 2016 and learned that although the telephone commonly travels throughout the valley on a daily basis, the telephone typically stays in the area of [redacted] overnight. It should be noted that although the telephone location information is not accurate enough to give the exact apartment number that the phone in located at in the [redacted] complex, the same complex as the [redacted]

58. On December 14, 2016, your Affiant conducted surveillance at the [redacted] and observed COSTANZO exit unit #202. COSTANZO was talking on a cell phone and appeared to lock the front door of the [redacted] with a key. COSTANZO then walked down the stairs and left the area on his bicycle. Investigators followed COSTANZO as he rode his bicycle to a restaurant in Mesa. COSTANZO entered the restaurant and was observed meeting with an unidentified male subject. Investigators overheard COSTANZO talking about Bitcoin, how banks are evil, and how the unidentified male's bank accounts had been frozen. Investigators also observed the unidentified male hand an unknown amount of U.S. Currency (large folded up handful of cash) to COSTANZO under the table. COSTANZO and the

unidentified male then appeared to conduct a transaction utilizing their cell phones. Investigators recognized this type of activity to be consistent with how COSTANZO has conducted Bitcoin transactions in the past. COSTANZO then left the area and Investigators followed him back to the [redacted]

59. On January 10, 2017, your Affiant reviewed the localbitcoins.com profile for Morpheus Titania (COSTANZO) and learned that he was still advertising the sale of Bitcoin for cash on the website and listing the same telephone number as his contact phone number for Bitcoin transactions.

60. On January 12, 2017, the Honorable John Z. Boyle, United States Magistrate Judge signed an extension to Order 16-543MB; authorizing the release of location information and the use of signal tracking technology on cellular telephone 602-434-1725 between January 12, 2017 and February 25, 2017. Your Affiant obtained and reviewed the location tracking information for the telephone from January 20, 2017 through January 26, 2017, and again from February 1, 2017 through February 4, 2017, our Affiant saw that the telephone continued to travel throughout the valley on a daily basis and typically stayed in the area of the [redacted] overnight. This further confirmed your Affiant's belief that COSTANZO lives at the [redacted] as previously observed during surveillance.

61. On February 2, 2017, your Affiant, acting in a UC capacity, contacted COSTANZO at his telephone number and arranged a third Bitcoin purchase from COSTANZO in the amount of $30,000. Your Affiant met with COSTANZO at a public venue in Tempe, Arizona. During the transacting, COSTANZO explained to your Affiant that he has a "banker" who he uses to help facilitate his larger deals. COSTANZO said that his "banker" will loan him thousands of dollars in Bitcoin whenever he needs it. Based on the prior UC meetings with COSTANZO including the IRS meetings with COSTANZO and STEINMETZ, your Affiant believes that the "banker" COSTANZO was referring to is STEINMETZ. Your

Affiant explained to COSTANZO that he is looking to exchange in excess of $100,000 for Bitcoin in the future and that the $30,000 transaction on that day was just a starting point. COSTANZO stated that he would need to make a couple calls to his "bank" to get the Bitcoin transferred for the deal and also mentioned that he has a person who wanted to purchase $14,000 in Bitcoin from him the next day.

62. Your Affiant sat with COSTANZO as COSTANZO appeared to send a couple of text messages. After approximately 10 minutes, COSTANZO advised that the Bitcoin had been transferred into his account and he could now complete the $30,000 transaction. While sitting with COSTANZO, COSTANZO further explained to your Affiant how he used to launder his cash Bitcoin proceeds through a Casino to exchange his $20's for $100's, but had to stop after he refused to give the casino his personal information (identification, social security number) and got thrown out.

63. Before completing the $30,000 transaction with COSTANZO, your Affiant spoke to COSTANZO about doing a $100,000 deal in the future. Your Affiant told COSTANZO that the $30,000 that was being utilized for the current transaction was proceeds from one kilo of cocaine. After hearing this, COSTANZO put his finger over his lips and said "shhh I don't want to know that." Your Affiant told COSTANZO that if he does three or four in the future (meaning sell three or four kilos of cocaine) that would be $100,000 in Bitcoin to sell. COSTANZO then completed the sale of approximately $30,000 worth of Bitcoin to your Affiant utilizing his cellphone to complete the transaction.

64. While waiting for the transaction to complete, your Affiant discussed with COSTANZO how a $100,000 transaction would occur in the future. COSTANZO advised that conducting the transaction is not a problem, but stated the issue with larger transactions is getting the cash onto the Bitcoin exchange to purchase more Bitcoin without setting off any red flags. COSTANZO said this is because a lot of the cash wire transfers are going out of the country because they go to Bitcoin

exchanges based in other countries. COSTANZO said that he could still conduct a $100,000 transaction, but would need time to make sure he can accrue all of the Bitcoin to sell. Your Affiant believes that when COSTANZO stated he needed to accrue all the Bitcoin, he was referring to meeting with STEINMETZ to get such a large amount. COSTANZO also told your Affiant to download a cellphone application called "Telegram" to communicate with him in the future. COSTANZO advised that Telegram is a secure messaging application he uses on his cellphone that "keeps the numbers off a server" and that your Affiant could search for his phone number on the Telegram application to contact him. COSTANZO and your Affiant agreed that they would communicate in the future about the upcoming $100,000 Bitcoin deal.

65. After completing the UC transaction with COSTANZO, your Affiant reviewed the location tracking information for COSTANZO's telephone. The location tracking data showed that the telephone was pinging at the location of the UC deal on February 2, 2017, throughout the entirety of the UC deal. This further confirmed your Affiants belief that COSTANZO controls the telephone and utilizes the phone to conduct his illicit transactions.

66. On February 23, 2017, the Honorable David K. Duncan, United States Magistrate Judge authorized a second extension of Order 16-543MB, authorizing the release of location information and the use of signal tracking technology on cellular telephone 602-434-1725 between February 23, 2017, and April 8, 2017. Your Affiant obtained and reviewed the location tracking information for the telephone from March 1, 2017, through March 3, 2017, and learned that the telephone continued to travel throughout the valley on a daily basis and typically stayed overnight in the area of the [redacted] This further confirmed your Affiants belief that COSTANZO continues to live at the [redacted]

67. On March 28, 2017, your Affiant reviewed the localbitcoins.com profile of Morpheus Titania (Thomas COSTANZO) and learned that COSTANZO was

continuing to advertise the sale of Bitcoin in exchange for cash on the website and that his contact phone number was still listed as (602) 434-1725. The webpage showed that COSTANZO had been active on the website on that same day.

68. On March 29, 2017, your Affiant contacted COSTANZO at his cell phone (602) 434-1725 to discuss the details of a future $100,000 Bitcoin transaction. Your Affiant sent COSTANZO a text message stating, "my guy wants me to send him 100k in Bitcoin either next week or the week after. Can you go that high." COSTANZO replied, "Sometimes," then told your Affiant to switch to the Telegram messaging application that he previously described during the UC meeting on February 2, 2017. COSTANZO sent your Affiant a message from the Telegram application utilizing his same telephone contact number. COSTANZO asked if your Affiant would be paying in cash and if we could do the deal this week. Your Affiant informed COSTANZO that the deal would be for $100,000 in cash and that it would be a week or two before the cash would be ready because it was coming from a third party. Your Affiant informed COSTANZO that he would talk to his "guy" and get more details about when the cash would be ready. COSTANZO expressed a willingness to conduct the transaction. COSTANZO explained that he would be using his "banker" to finance this transaction because he does not have such a large amount of Bitcoin on hand. Based on the prior UC meetings with COSTANZO, including the IRS meetings with COSTANZO and STEINMETZ, your Affiant believes that the "banker" COSTANZO was referring to is STEINMETZ. It should be noted that during the UC transaction conducted on February 2, 2017, your Affiant advised COSTANZO that the $100,000 transaction they were planning to conduct would be from the proceeds of cocaine sales.

69. Between March 29, 2017, and April 10, 2017, your Affiant continued to communicate with COSTANZO via the Telegram application and coordinated a meeting with COSTANZO and his "banker" (which was later identified as STEINMETZ) to discuss the terms of a $100,000 Bitcoin purchase in which

STEINMETZ would be the source of supply for the Bitcoin. The meeting between your Affiant, COSTANZO, and STEINMETZ was arranged for April 10, 2017.

70. On April 10, 2017, members of TFG1 conducted a covert operation at a public venue in Tempe, Arizona. Your Affiant, acting in a UC capacity, met with COSTANZO and STEINMETZ to discuss the details of the $100,000 Bitcoin purchase. Your Affiant sat at an outside table and waited for COSTANZO and his "banker" to arrive. COSTANZO arrived in a brown passenger car and backed into a parking space, obscuring his license plate. COSTANZO exited the vehicle and walked into the venue, advising your Affiant that he was going to get a coffee. Approximately one minute later, your Affiant observed STEINMETZ approach the venue from south side of the building. Your Affiant recognized STEINMETZ based on his Arizona Motor Vehicle Department (MVD) photograph and a photograph that was posted of STEINMETZ on http://steinmetz.org/peter. STEINMETZ walked into the venue and met with COSTANZO. It was later learned that STEINMETZ arrived to the meeting location driving his red **Porsche Boxster** bearing Arizona license plate "SATOSHI." An Arizona MVD query on the **Porsche Boxster** revealed that the vehicle was 2000 **Porsche Boxster**, red-in-color, bearing Arizona license plate "SATOSHI," assigned VIN: [redacted], registered to Peter STEINMETZ at [redacted]

71. A few minutes later, COSTANZO and STEINMETZ exited the venue and sat with your Affiant at the outside table. STEINMETZ introduced himself as "Amideo," and never provided his true name. COSTANZO continued to refer to himself as "Morpheus". Throughout the meeting, COSTANZO and STEINMETZ mentioned that they had been conducting business together since 2013. STEINMETZ confirmed that he believes they conducted their first deal together in April 2013. COSTANZO advised that "the other day" he did his first deal where he purchased "Bitcoin, Ethereum, and Dash" all at the same time. Your Affiant recognized that

Ethereum and Dash are other types of digital currencies known as Altcoins that can be used as a store of value or as a method of payment much like Bitcoin.

72. Your Affiant explained to STEINMETZ a need to purchase large amounts of Bitcoin to transport currency across state lines. Your Affiant explained that he has a business partner in California and that their business takes in large amounts of cash from sales. Your Affiant advised that he needs a good way to transport the currency rather than driving the cash from state to state. Your Affiant advised that the last thing your Affiant needs is to get stopped by the police and have to explain the origin money. STIENMETZ interjected and said "they will just seize it all." STEINMETZ then spoke about civil asset forfeiture and said that the problem with forfeiture is that if your money is seized, there is only a small possibility of getting your money back through a court process. STEINMETZ then suggested that your Affiant go home and write an email to Governor Ducey because he believes there is a bill currently in front of Governor Ducey to change the civil asset forfeiture laws in Arizona.

73. STEINMETZ stated that he could certainly sell your Affiant $100,000 worth of Bitcoin, but advised that he wants his deal to be legal. STEINMETZ stated that he wanted to be assured that the money used for the deal is not illegal proceeds and advised that he might need to see some identification in case he is ever questioned about who he got the money from. STEINMETZ stated that he makes some money from the business transaction but does not want to put himself at risk with the law. STEINMETZ made it clear that he does not file any paperwork, complete any government documentation, or distribute any personal information about the transaction unless he is required to by a court subpoena. STEINMETZ advised that the only way he would even speak to law enforcement would be in the presence of his attorney with a court subpoena. STEINMETZ said that this is always his position.

74. Your Affiant explained to STEINMETZ that he does not want any government documentation about the transaction and wanted to ensure there is no bank

reporting like what would occur at Wells Fargo if someone went in with $100,000 cash. STEINMETZ said that he knows exactly what would happen at a bank if someone came in with that much cash and said that they would file two forms. He advised that one form (STEINMETZ could not remember the exact form number) is for anytime someone deposits over $10,000 cash and the other form is called a Suspicious Activity Report (SAR). STEINMETZ said the he probably gets those forms filed on him all the time. He advised that the forms get sent to FinCEN which he explained stands for financial crimes enforcement. STIENMETZ further explained that he does a fair amount of cash business and advised that if he goes to a bank more than once every two weeks with more than $10,000, he believes there is a whole department that handles that type of activity which he explained is virtually an instrument for the government.

75. STEINMETZ said that he has some customers who want to remain anonymous. He said that these customers sometimes purchase gold, then he sells them Bitcoin for their gold bars. He advised that he does not even consider that a currency transaction.

76. Your Affiant expressed concerns to STEINMETZ about his request to take a photograph of your Affiants identification. STEINMETZ advised that he would never release the information to anyone without a court order. STEINMETZ said that he keeps the documents secured in his safe at home and no one will ever see them. STEINMETZ also stated that he keeps records of all the deals he does, but as far as he is concerned, he does not even remember doing the deals.

77. STEINMETZ then discussed the details of how the $100,000 deal would occur. Your Affiant advised that it would be preferable to conduct the transaction on the Monday or Tuesday (April 17th or 18th) because your Affiant would be collecting the cash over the weekend. STEINMETZ said that he would only need a few days heads-up to assure he has the Bitcoin and that it will be available when your Affiant needs it. It was also decided that the deal would occur at the Chandler airport. STEINMETZ stated that he is a pilot and flies his own plane.

STEINMETZ stated that he has access to the pilots lounge at the airport and would prefer to conduct the deal there rather than in a parking lot somewhere where the police might see the deal. STEINMETZ also stated that he would be armed during the deal for everyone's safety.

78. STEINMETZ informed your Affiant that he and COSTANZO are fairly well-known in the Bitcoin community and that there was no reason to be concerned about the deal. Your Affiant verified that STEINMETZ would be charging a 7 percent fee above the average market price of Bitcoin to conduct the transaction. STEINMETZ confirmed the fee and said that he and COSTANZO would be splitting the proceeds from the transaction. STEINMETZ advised that he had another appointment on Monday morning, but that the transaction could still be conducted on Monday afternoon or Tuesday morning. STEINMETZ again confirmed that the deal would be conducted at the Chandler Municipal Airport in one of the pilot rooms. He advised that there would be no security checks to get into the room and that it would not look out of the ordinary to conduct a deal in the room. It was agreed that COSTANZO and STEINMETZ would chose the specific pilot room to meet, bring a money counter and computer for the deal, and inform your Affiant which room to meet in.

79. Before the meeting was concluded, STEINMETZ mentioned that one of the craziest deals he ever conducted was on a dark street in downtown Phoenix. He said that it was with someone he trusted and advised that he has never had a deal go bad and does not plan on ever having a deal go bad. STEINMETZ told your Affiant to contact COSTANZO when your Affiant is ready to do the deal and that COSTANZO will coordinate the deal.

80. At the conclusion of the meeting, as your Affiant was leaving the venue, your Affiant observed STEINMETZ's red **Porsche Boxster** displaying Arizona license plate "SATOSHI" parked on the east side of the building. This confirmed your Affiants belief that STEINMETZ utilizes the **Porsche Boxster** to facilitate his illegal Bitcoin exchange business.

81. Your Affiant believes based on the investigation, including the undercover meetings with COSTANZO and STEINMETZ and their own statements that these individuals are knowingly operating an unlicensed money transmission business and laundering proceeds from illegal activities including drug trafficking by exchanging U.S. Currency/cash for Bitcoin. Based on statements made by COSTANZO, your Affiant believes that COSTANZO stores his proceeds from exchanging and/or money laundering cash for Bitcoin in multiple forms of currency including Bitcoin, precious metals (gold and silver), and cash. Your Affiant believes that since both COSTANZO and STEINMETZ do not trust banks or agree with government regulations, that they store at least a portion of the illicit proceeds obtained from their business at their residences, the [redacted] Your Affiant further knows that COSTANZO and STEINMETZ utilize electronic communication devices including cellphones to initiate, facilitate, and conduct their currency exchange services. Your Affiant believes based on the amount of cash transactions COSTANZO and STEINMETZ conduct on any given day (as explained during the meetings with both COSTANZO and STEINMETZ) that they are concealing a large amount of United States currency unreported to the United States government at both the [redacted]

NECESSITY FOR ANALYSIS OF ELECTRONIC DEVICES

82. Your Affiant is aware that this investigation involves the peer-to-peer exchange of Bitcoin, which is conducted between at least two individuals each using an electronic device such as a smart cellular telephone, computer, laptop, and/or electronic tablet (hereinafter referred to as "electronic devices"). Electronic digital currency can be accessed, manipulated, and stored on electronic devices. Bitcoin exchangers advertise their services on websites on the internet which are also accessed via electronic devices. Your Affiant knowns that Bitcoin exchangers and

their customers, in efforts to conceal their activity and remain undetected, communicate through encrypted communication applications that must be downloaded to electronic devices equipped with the proper technology to run the applications' software. Your Affiant knows that both COSTANZO and STEINMETZ have used or made mention of using electronic devices to conduct the exchange of Bitcoin for case. They have both been observed conducting transactions using a cellular telephone device and are planning on using a computer/laptop to conduct the $100,000 exchange in the near future with your Affiant who is acting in a UC capacity. Additionally, both COSTANZO and STEINMETZ have taken steps to conceal their true identity by using an alias and communicating with encrypted messaging systems.

83. Based on your Affiants training and experience, your Affiant is aware that encrypted systems and other hidden anonymizing services can be accessed open source but are also highly accessed on the Darknet via a special web browser known as "The Onion Router" (TOR). TOR utilizes multiple Internet Protocol (IP) relays to obscure a person's IP address and the physical location of that IP address while using the network. Your Affiant knows that a common computer operating system used for this type of anonymous Darknet activity is called the "TAILS" operating system. TAILS is a "live operating system" and can be contained on a USB stick, SD card, or DVD. The TAILS system allows users to browse the internet anonymously through TOR and will immediately delete all record of the computers history including messaging, email, and internet history as soon as the device is shut down. Your Affiant knows that users of this technology are typically savvy when it comes to digital security and remaining anonymous.

84. Your Affiant is further aware that the TOR browser, as well as access to most electronic Bitcoin accounts can be accessed through cell phones, computers, and tablet devices. Since Investigators have identified that Bitcoin is the primary form of digital asset used during this investigation, your Affiant believes that "Digital Bitcoin Wallets" and other incriminating digital information logs may be located

on multiple computers, cell phones, and tablets located during the execution of the search warrant.

85. Based on the information from this investigation, your Affiant believes that electronic evidence including computers, cell phones, tablets, and digital storage devices that are being used to facilitate, process, conceal, and document Bitcoin transactions will be located on COSTANZO's person, in COSTANZO'S [redacted] on STEINMETZ' person, in STEINMETZ' [redacted] and in STEINMETZ' **Porsche Boxter**. Your Affiant further believes that said electronic devices located at the locations described in this Affidavit are being utilized to store digital Bitcoin wallets containing proceeds from the unlawful exchange of Bitcoin or the laundering of United States currency. Your Affiant also believes that said electronic devices contain ledgers and information documenting details of transactions involving the unlawful exchange of Bitcoin or the laundering of United States currency. Such electronic devices can contain processors, are easily transportable, small in size, store a lot of information, and are capable of securing and encrypting information essential to facilitating a Bitcoin transaction.

86. Your Affiant knows based on training, experience, and knowledge of this investigation that it is possible for co-conspirators who may be unknown to Investigators at the time this warrant is served, to remotely access electronic devices including computers, cell phones, and tables to alter digital evidence, or entirely remove digital evidence and/or proceeds from said devices for amongst other reasons to destroy inculpating evidence and avoid the seizure of proceeds.

87. Your Affiant submits that if a computer, laptop, cellular telephone, tablet, or other digital storage medium and/or electronic device is found at any of the locations described within this Affidavit, or in the possession of COSTANZO or STEINMETZ at the time of their arrest, that there is probable cause to believe records described in Attachment B and Attachment C will be stored on that computer, laptop, cellular telephone, tablet, or other digital storage medium and/or

electronic device. Due to the nature of this investigation and based on the exigency that digital forensic evidence may be lost if not immediately analyzed, your Affiant requests that this application allows for Investigators to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers, laptops, cellular telephones, tablets, or other digital storage mediums and/or electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer, cell phone, or tablet located because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of

malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

88. *Necessity of seizing or copying entire computers, cell phones, tablets, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of

storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

89. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant your Affiant is applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant and in Attachment B, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

90. Based on the aforementioned, your Affiant respectfully submits that there is probable cause to believe there have been violations of federal law, specifically, violations of Title 18 U.S.C. §§ 371 and 1960(a) (Conspiracy to operate unlicensed money transmitting business), 18 U.S.C. §§1960(a) and 1960(b)(1)(B) (Operation of unlicensed money transmitting business), 18 U.S.C. 1956(a)(3)(B) (Money laundering to conceal or disguise the nature, location, source, or ownership of proceeds represented by a law enforcement officer to be proceeds of drug trafficking in violation of 21 U.S.C. §§ 841 and 846), and 18 U.S.C. 1956(a)(3)(C) (Money laundering to avoid transaction reporting requirements of proceeds represented by a law enforcement officer to be proceeds of drug trafficking in violation of 21 U.S.C. §§ 841 and 846). Furthermore, your Affiant respectfully submits that there is probable cause to search:

a) AN APARTMENT UNIT located at [redacted] as described in attachment A-1. This is a multi-unit, two

story apartment complex located on [redacted] is located on the second story, far south end of the complex. Unit [redacted] is the first unit located at the top of the most southern staircase. The front door to the unit faces west and has a tan in color metal security door. At the time of this writing, there is a piece of white paper in the front window to the unit with the numbers [redacted]" printed in black.

b) A RESIDENCE located at [redacted] as described in attachment A-2. This is a single story residence with a tan brick exterior and a brown shingle roof. [redacted] Peter STEINMETZ as the owner of the property. (Further identified in attachment A-2)

c) The VEHICLE identified as a 2000 **Porsche Boxster**, red in color, displaying Arizona license plate "SATOSHI", assigned VIN: [redacted] currently registered to Peter STEINMETZ at [redacted] (hereinafter referred to as "**Porsche Boxster**"), as described in attachment A-3.

91. Furthermore, pursuant to Title 18 U.S.C. § 982 (Criminal forfeiture), incorporating the procedures governing forfeitures for violations of Title 18 U.S.C. §§1956(a)(3)(B), 1956(a)(3)(C), 1960(a), and 371, your Affiant further submits that there is probable cause for the seizure and forfeiture of the following vehicle:

a) The **Porsche Boxster** referred to as above, which is specifically identified as a 2000 **Porsche Boxster**, red-in-color, displaying Arizona license plate "SATOSHI", assigned VIN: [redacted] currently registered to Peter STEINMETZ at [redacted]

(hereinafter referred to as "**Porsche Boxster**"), as described in attachment A-3.

Pursuant to 28 U.S.C. §1746(2), I declare under penalty of perjury that the foregoing is true and correct.

Chad Martin, Task Force Officer
United States Drug Enforcement Administration

Subscribed and sworn to before me on the 13th day of April, 2017.

~~HONORABLE JOHN Z. BOYLE~~
~~United States Magistrate Judge~~

DAVID K. DUNCAN
U.S. Magistrate Judge

EXHIBIT

B

Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

SEALED

In the Matter of the Search of
(Briefly Describe the property to be searched or identify the person by name and address

[redacted]

Case No. 17- 6138MB

(Filed Under Seal)

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Task Force Officer, Chad Martin, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

As further described in Attachment A-1.

Located in the District of Arizona, there is now concealed (*identify the person or describe the property to be seized*):
The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

AS SET FORTH IN ATTACHMENT B AND ATTACHMENT C.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	Offense Description
18/371, 1960(a)	Conspiracy to Operate Unlicensed Money Transmitting Business
18/1960(a), (b)(1)(B)	Operation of Unlicensed Money Transmitting Business
18/1956(a)(3)(B)	Money Laundering to Conceal or Disguise
18/1956(a)(3)(C)	Money Laundering to Avoid Reporting Requirement

The application is based on the facts contained in the attached Affidavit of Task Force Officer Chad Martin.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Carolina Escalante Konti

Applicant's Signature

DEA Task Force Officer Chad Martin
Printed name and title

Date and time issued: Apr. 19, 2017

Judge's signature

City and State: Phoenix, Arizona

Honorable ~~John Z. Boyle~~ David K. Duncan, United States Magistrate Judge
Printed name and title

EXHIBIT

C

ATTACHMENT B

THINGS TO BE SEARCHED FOR AND SEIZED

EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF CRIMINAL OFFENSES

Agents are authorized to search for and seize evidence of violations of Title 18 U.S.C. §1956(a)(3)(B) and (C) (Conceal or disguise the nature, location, source, or ownership of proceeds of unlawful activity being represented by a law enforcement officer)(Avoid transaction reporting requirements), Title 18 U.S.C. §1960 (Operation of unlicensed money transmitting business), and Title 21 U.S.C. §846 (Conspiracy to Distribute a Controlled Substance);

1. Heroin, Cocaine, Methamphetamine, or any other illicit drug.
2. United States Currency or currency of any nation, coins, precious metals, Digital currency including Bitcoin, Ethereum, Dash, or other digital coin "altcoin", and any other financial instruments believed to be proceeds of money laundering or drug sales, including any containers, devices, or secret compartments capable of holding the same.
3. Bank documents and records, financial documents and records, and any and all records and documents relating to any bank or financial transactions, including ~~but not limited to~~: digital Bitcoin transactions, correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly and/or periodic account statements for all such accounts; copies of check journals, check ledgers, checkbooks, deposit

tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, and/or any related financial statements, and/or mortgage and/or promissory notes for all such accounts; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts, with associated copies of canceled checks, check registers, safe deposit box records and keys, wire transfer receipts, money order receipts and purchases, and records relating to employment, wages earned and paid, business income earned, and other compensation records.

4. Books, records, receipts, notes, ledgers, correspondence and other papers relating to the transportation, ordering, purchase, and distribution of controlled substances, or the laundering of proceeds.

5. Any and all monetary related customer lists, dealer lists, or any notes containing the individual names of such persons, telephone numbers and/or addresses of these customers or dealers, any corresponding records of accounts receivable, money paid or received, drug supplied or received, cash supplied or received, and digital currency supplied or received.

6. Papers, tickets, notes, receipts, and other items relating to domestic and international travel, including ~~but not limited to~~, appointment calendars, receipts, notes, letters, airline tickets, bus tickets, food receipts, hotels, and/or other lodging receipts, related correspondence, envelopes, and opened and unopened mail.

7. Books, records, invoices, receipts, correspondence, records of real estate transactions

and documents showing ownership of real estate, vehicles, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashiers' checks, bank checks, loan applications, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfers, concealment and/or expenditure of money.

8. Address and/or telephone books, Rolodex indices and any papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists or which indicate a criminal association between co-conspirators.

9. Indicia of occupancy, residency, rental and/or ownership of the premises described herein, including, utility and telephone bills, canceled envelopes, rental purchase or lease agreements, and keys.

10. Indicia of ownership or control over any vehicles or aircraft including, ~~but not limited to,~~ titles, registrations, receipts, repair bills, and keys belonging to that vehicle.

11. Items and/or documents evidencing the expenditure of the proceeds of money laundering or drug distribution including, ~~but not limited~~ to, real estate, vehicles, aircraft, clothing, furniture, jewelry, art work, and electronic equipment.

12. Copies of income tax returns, workpapers, profit and loss statements, and related correspondence concerning Thomas COSTANZO or Peter STEINMETZ and any

other entities under the name of Thomas COSTANZO, Peter STEINMETZ, Morpheus Titania, or Amideo.

13. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

14. Any telephone, cellular telephone, tablet, computer, USB storage device, electronic digital currency storage devices, or digital display device found in the locations to be searched, including any electronically stored data found in the same, including, ~~but not limited to, data~~ regarding outgoing calls, incoming calls, missed calls, phone book memory data, contact names and numbers, call details including call history, electronic mail (email) messages, text messages and text message history, encrypted messaging applications, virtual currency applications, crypto-currency wallet applications, and all digital images, as well as listening to, noting and recording any messages or recordings left on any telephone answering device or recording device found in the location to be searched.

15. ~~Firearms and ammunition, including handguns, pistols, revolvers, rifles, shotguns, machine-guns and other weapons purchased with illegal proceeds and/or used~~ to protect and facilitate illegal currency transactions, ~~and any records or receipts~~ pertaining to firearms and ammunition.

16. Photographs, identification cards, address books or similar items which indicate a criminal association between co-conspirators.

THIS CATEGORY IS NOW AMENDED BY 4/20/17 4:30 P.M. PURSUANT TO 4 DAY TELEPHONIC AND RECORDED AMENDED TESTIMONY TAKEN 4/20/17 AT 4:15 P.M. AND TRANSMITTED TO THE CLERK FOR PREPARATION OF A MODIFIED, ANSWERS TO REQ.

17. Packaging material, shipping material, shipping labels, shipping postage, and any other paraphernalia related to the use and/or distribution of controlled substances.

18. Drug paraphernalia or other items used for possessing, processing, testing, packaging, weighing, transporting, concealing, purchasing, selling, or ingesting illegal controlled substances.

19. Safes or storage containers where co-conspirators would store, place, or keep records, documents, and/or information of illegal business transactions.

20. For any computer, computer hard drive, external hard drives, disk, USB data stick, electronic digital currency storage device, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, and browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. Evidence of the lack of such malicious software;

d. Evidence of communication on TOR darknet websites and the use of the digital crypto-currency Bitcoin or other "Altcoin";

e. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. Evidence of the times the COMPUTER was used;

h. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. Documentation and manuals that may be necessary to access the COMPUTER or conduct an examination of the COMPUTER;

j. Contextual information necessary to understand the evidence described in this attachment;

k. Computer software which may have been used to create, access, modify or to otherwise interact with the stored files. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. It commonly includes the operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;

l. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment,

modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.

m. Records and things evidencing the use of the Internet to facilitate the distribution of illicit drugs and laundering of monetary instruments, including:

i. Routers, modem, and network equipment used to connect computers to the Internet;

ii. Records of Internet Protocol addresses used;

iii. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used herein, the terms "records," "documents," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); and any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing).

Furthermore, all electronic items listed above may be searched, examined, and/or imaged by investigators forensically to obtain information related to items described above. Reference is made to ATTACHMENT C for further information on the technical examination of electronic devices.

ATTACHMENT C

TECHNICAL TERMS

1. Based on your Affiants training and experience, I use the following technical terms to convey the following meanings:

a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

2. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

3. Your Affiant submits that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

4. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

5. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss

of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

6. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

EXHIBIT

D

Mr. Steinmetz: I don't know, but I would imagine they did. I mean, I have no idea.

Male voice: I never assumed, I would never do one, you know, for that reason I would never deposit one you know, like $9,000.

Mr. Steinmetz: I know, but if you deliberately break up your deposits into less than $10,000, you are guilty of the federal crime of structuring your deposits. [Laughter.]

IRS SA: I think that's another, that probably attracts attention. You go to keep going with $9,000 deposits every, there, you know.

Male voice: I wouldn't know anything.

Mr. Steinmetz: It's just, you know, I have a…

Male voice: You know I mean, I have privy to an attorney so I've asked him where my money's coming from.

IRS SA: Good, yeah.

Mr. Steinmetz: I'm on, you know, I mean Alex and I are going through all this game up on any attempt at add on with the bit point stock. So, you know, I'm a well-known member of the community. They can find me. They know where I live.

IRS SA: Right.

Mr. Steinmetz: You know, they, they want to come and get me, they can. So I just try to keep all my stuff legal.

Wait staff: Are you drinking?

IRS SA: Right. You know, I get a slice and a diet coke.

Wait staff: All right, a slice of what?

Mr. Steinmetz: You know, if somebody comes up to me and says you know, you got this money, it's from somebody with no identity…

IRS SA: Um, just do the pepperoni.

Wait staff: There's a two-slice special. Two slices and a coke for $6 bucks.

IRS SA: Oh that sounds like a plan, I'll take that.

Wait staff: All right.

Mr. Steinmetz: If you tell me outright that what you're doing is illegal, then I'm sorry, I can't be

EXHIBIT

E

Q: Then put them on my phone. Is there any way, like, the government can find out what we did or track that or...

A: It could be done. Uh, okay, think of Bitcoin as pseudo anonymous. It's not 100% anonymous.

Q: Okay.

A: But it - it - it even - it - it takes a lot of energy...

Q: Yeah.

A: ...to determine who has them or w- you know, to track them. Because what happens is, like...

Q: Yeah, but they have...

A: ...for example...

Q: Say you got a guy, (Pete), and he's got a million dollars cash and he can get all his Bitcoins and send 'em to you.

A: Yes.

Q: Is there any way the government can find out you have them?

A: It's very difficult. It's very difficult because the way this works is with - with - with the application that I us and most applications today - these days, uh, I use Mycelium. I like it the best.

Q: Okay.

A: Uh, but there's other ways, you know, if that's something that's very high on your priority list...

Q: Uh-huh.

A: ...there's ways to make it more ob- uh - uh - uh, sophisticate it more.

Q: Okay.

A: Okay, so for example - I don't know what you downloaded. Did you use...

Q: I got Blockchain...

A: Okay.

Q: ...and breadwallet.

A: Okay, yeah those are both good applications. I - I - I recommend them.

Q: Okay.

A: Um, for Apple I do recommend the - the breadwallet. Ah, if you're really super wantin' to be more, you know, sophisticated even more then you would use LocalBitcoins.

Q: Okay, so that...

((Crosstalk))

A: 'Cause LocalBitcoins...

Q: So there's not an app for that though. Is there?

A: Yeah, there is. Well there's not a...

Q: You have to go on the computer and do it.

A: On- online.

Q: Okay.

A: You can do it online. Um, but, uh, so what happens is - okay, let me just show you. So I have on this - in this account 13 Bitcoins on this account.

Q: Okay.

A: But if you go over here and you go - so once that output - so in this account right here I have 1000th of a Bitcoin. Another 1000th of a Bitcoin.

Q: So you just...

A: 6000th of a Bitcoin. Uh, 3000 - oh there are 10,000 - 100,000, uh, 600 point, uh, 7 - 10 point, uh, 200ths - 200ths, uh, 8, 3 are in all these address.

Q: So it's all, like, a like an address.

A: What - what...

Q: That's what these are? Like...

A: Yeah, what - what - what - what happens is...

Q: Or is that all in, like, (billions).

A: Yeah, what happens - and breadwallet does this too. What happens is when - if send you Bitcoins it's going to take Bitcoins from those different addresses and send 'em to you. Like...

Q: It will automatically, like, pulls it from all yours.

A: It pulls 'em from all...

Q: Okay, so that 13 is probably out - into all those addresses?

A: Right.

Q: Okay.

A: Right. So, like, for example. Let's see if I can find you one here. Let's see. I send - let's see what happens there (with these guys). Okay, so I sent, uh, I had 17 Bitcoins. Actually I sent these to myself. So what it does is it sends - I have 17 Bitcoins in one address and it send 8.39 to this address. And then this is my change address.

Q: Okay.

A: Okay, and it only uses this address one time unless I put more coins into that address for anything.

Q: Getting confusing. So that just helps, like, kinda hide 'em with different addresses?

A: Well what happens is that - let me see if I can find a better example. Let's see if I can find a better example.

Q: Okay.

A: So that's basically a million combinations you're gonna have to go through...

Q: Yeah.

A: ...in order to figure out what it is.

Q: So - and you can log in on another phone and...

A: I can go get 'em off - yeah, off the other phone, create a new account and then you - now I - I'm back in business.

Q: Okay.

A: So...

Q: So it's safer that way too 'cause no one can steal your stuff.

A: Right, it's - it's - the - the beauty behind the system is - god, I wanna show you one here and that really would ma- you know, show you what to ex- how this works. You know, uh, um, so I paid - I gave twen- I paid $25 to Gary Johnson with this. And I did it anonymously.

Q: Do we - how long does it take to do this. I don't want you to miss your movie.

A: Oh well - oh yeah, well - yeah - yeah, I'll just - yeah, we're writin' the same thing. Okay, but yeah, we got a few more minutes. I wanna show you one that actually shows a good - shows what, you know, this - this spreading out of all these - for whatever reason here I'm (unintelligible). I'm lookin' for one of the big ones. I mean, I have from

(unintelligible) (school). Okay, (alphabet). No. Okay.

Q: And do you have to...

A: So...

Q: ...tell it to do it from (unintelligible) or it's just automatic when that happens.

A: It does it automatically.

Q: That's on...

A: So - so in f- so, like, w- in this example, okay, I sent, uh, .224 Bitcoins or no. I sent 3.51 Bitcoins to this address I believe. I'd have to look at it. But what it did is it took Bitcoins from this address, this address, this address and then it send them to this address and then there's the change.

Q: Okay.

A: So it makes it very, very, very, very difficult...

Q: Yeah.

A: Because you're making a new address every time. And the number of addresses is, uh, 10 to the 68th power.

Q: Yeah, I know what you're (talking about).

A: So there's more - more - more - there's more addresses than there are quantum particles in the universe.

Q: Uh-huh.

A: So that way you can start gettin' really big numbers...

Q: Yeah.

A: It just gets big in a hurry.

Q: All right.

A: Like - like, the example is the shot 256, the - the - the system that does the - the mining...

Q: Uh-huh

A: ...is 2 to the 256th power. Now this is how big this number is. If you took the - the energy of the sun and you could harness all that energy, every ounce (drool) of energy that the sun was putting out and you ran it into a computer and the computer could handle all the energy that the sun was - was - was using.

Q: Okay.

A: The sun would burn out to - before the computer would count the 2 to the th 256th power.

Q: Well that's good. So their...

A: That's...

Q: We're never gonna run out.

EXHIBIT

F

A: I - don't - don't tell me that.

Q: Yeah.

A: You know, I don't need to know the information like that.

Q: Yeah.

A: Because w- what - what difference does it make to me?

Q: Yeah.

A: It's - it's...

Q: You're an...

A: ...none of my bus- it's none of my business. My business is - is anonymity and (speaking).

Q: Yep. Now do you know much - obviously you know - you know everything about Bitcoin. You know much about, like, darknet?

A: Um, I haven't really experimented too much.

Q: 'Cause that's what I'm tryin' to, I mean, I'm not tryin' to come out but some things I do we have to send products back and forth and then this - now I need a way to pay for it.

A: Yeah.

Q: And there's another way I - I've been learning about is to buy stuff on the darknet. They ship it to your house and you pay with Bitcoin.

A: Mm-hm.

Q: And I hear that's even more secure 'cause you don't have to - everything's - you can use different browsers and stuff where they...

A: Well...

Q: ...(IDUR)...

A: ...the problem is is that the - is that the failure of the system is that somebody takes down the website...

Q: Yeah.

A: ...then you're hosed.

Q: But...

A: With this system...

Q: I mean, I - how do you know how the website works right?

A: Well with what we're doing is the list level is super-duper low.

Q: Yeah.

A: Because I don't - I don't send you the - I don't send the Bitcoins 'til I get the money.

Q: Yep.

A: And once I send 'em bam they're there. There is no customer service.

Q: Yeah. But well isn't there a verification pro...

A: Yeah, I mean, I'll show you how that works once you actually probably do this deal.

Q: Okay.

A: 'Cause I gotta - I told my girlfriend I'd meet her at, uh, 7 o'clock. So, um...

Q: I don't know how you do the money.

A: Oh yeah just give it to me.

((Crosstalk))

A: Yeah, (unintelligible).

Q: That's what I got.

A: Um, so right now we're at, uh, 50-14-84. And I'll show you where the number lay. So 681 - 8 (unintelligible) 6 - 614-84...

Q: So that - that's just, like, a general (estimate)?

A: This is on BitcoinAverage. That's what I - that's what everybody uses. Not everybody - most people. It's a compilation of all the different exchanges.

Q: So they can average price...

A: Average without - it's weighted.

EXHIBIT

G

WIRED https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

AUTHOR: ANDY GREENBERG

SECURITY

11.07.14 06:00 AM

GLOBAL WEB CRACKDOWN ARRESTS 17, SEIZES HUNDREDS OF DARK NET DOMAINS

When "Operation Onymous" first came to light yesterday, it looked like a targeted strike against a few high value targets in the Dark Web drug trade. Now the full scope of that international law enforcement crackdown has been revealed, and it's a scorched-earth purge of the Internet underground.

On Friday, the European police agency Europol along with the FBI and the Department of Homeland Security announced that the operation has now arrested 17 people in as many countries and seized hundreds of Dark Web domains associated with well over a dozen black market websites. In addition to the takedowns of drug markets Silk Road 2, Cloud 9 and Hydra revealed Thursday, it's also busted contraband markets like Pandora, Blue Sky, Topix, Flugsvamp, Cannabis Road, and Black Market. Other takedown targets included money laundering sites like Cash Machine, Cash Flow, Golden Nugget and Fast Cash. And agents have taken from criminal suspects more than $1 million in bitcoin, $250,000 in cash, as well as an assortment of computers, drugs, gold, silver and weapons that they had yet to fully catalogue.

In all, the agency says it's seized 414 ".onion" domains, the web addresses used by the anonymity software Tor that hides the physical location of those sites' servers. When WIRED spoke Thursday night with Troels Oerting, head of the European Cybercrime Center, he said his staff hadn't even had time to assemble the full list of sites it's pulled down in the sprawling operation.

"One of the primary targets was the Silk Road guy," said Oerting, referring to Blake Benthall, the 26-year old coder arrested in San Francisco Wednesday and accused of managing the popular Silk Road 2 drug site. "But we also decided to see if we could identify more of the administrators of these sites and remove their infrastructure as well...Some moved before we could act, but we've taken most of our targets down."

Europol didn't immediately share the details of the 17 arrests related to the operation. But aside from Benthall, it revealed earlier on Thursday that two individuals had been arrested in Dublin in a large Dark Web-related drug bust.

Just how law enforcement agents were able to locate the Dark Web sites despite their use of the Tor anonymity software remains a looming mystery. In its criminal complaint against Benthall, for instance, FBI agent Vincent D'Agostini writes merely that in May of 2014 the FBI "identified a server located in a foreign country believed to be hosting the Silk Road 2.0 website at the time," without explaining how it bypassed Tor's protections. The sheer number of Tor-hosted sites affected by the takedown raises

questions about whether law enforcement officials may have found new vulnerabilities in Tor's well-tested anonymity shield.

Asked how Operation Onymous located the sites, Europol's Oerting was unapologetically secretive. "This is something we want to keep for ourselves," he said. "The way we do this, we can't share with the whole world, because we want to do it again and again and again."

The organization that created and maintains Tor, the non-profit Tor project, said it didn't have any more information on Operation Onymous' techniques. But it downplayed the threat of a vulnerability in Tor's safeguards for the tough-to-trace sites it protects known as Tor hidden services. "It sounds like old-fashioned police work continues to be effective," said Andrew Lewman. "It could be [that law enforcement targeted] common people or organizations running these hidden services, or a hosting company, or something more mundane than a hidden service exploit."

The sheer number of Tor-hosted sites affected by the takedown raises questions about whether law enforcement officials may have found new vulnerabilities in Tor's well-tested anonymity shield.

Despite whatever tricks Europol and its American counterparts used to unmask the sites, several of the most popular Dark Web drug markets have nonetheless eluded them. A study by the non-profit Digital Citizens Alliance in September found that the six most popular Tor-based markets by total product listings were Silk Road 2, Agora, Evolution, Pandora, Andromeda, and BlueSky. Operation Onymous captured fully half of those top sites. But Agora, Evolution and Andromeda remain online and will likely absorb many of the refugee buyers and sellers from the law enforcement busts. In fact, Agora had already passed the Silk Road in total product listings with more than 16,000 mostly-illegal offerings, and the fast-growing marketplace Evolution was already on pace to soon take the second place spot in the underground economy.

Operation Onymous comes just over a year after the takedown of the original Silk Road drug site and the arrest of its alleged creator Ross Ulbricht, whose trial is scheduled for January. In an open letter to Attorney General Eric Holder just last week, New York Senator Charles Schumer called for a renewed crackdown on the flourishing Dark Web sites that have filled the void left by the original Silk Road. He pointed to statistics that show that more than twice as many drugs are now being sold on the Dark Web compared to when the original Silk Road was online.

Though Operation Onymous left many of that underground economy's major players intact, Europol's Oerting said he was more confident than ever that the remaining sites can be tracked down and pulled off the Internet.

"This is just the beginning of our work. We will hunt these sites down all the time now," he said, praising the cooperation of all the international law enforcement agencies involved. "We've proven we can work together now, and we're a well-oiled machine. It won't be risk-free to run services like this anymore."

#DARK WEB#DRUGS#SILK ROAD#TOR

EXHIBIT

H

1092		
1093	A:	That sounds good.
1094		
1095	A5:	Okay.
1096		
1097	A:	Just got it in a baggie for ya.
1098		
1099	A5:	All right. (Unintelligible).
1100		
1101	A:	I - I got the big bills, like, yup...
1102		
1103	A5:	Thank you.
1104		
1105	A:	I find big bills are better so that...
1106		
1107	A5:	Well it's just...
1108		
1109	A:	Obviously it's easier (unintelligible).
1110		
1111	A5:	I had the other day this guy he, uh, he buys a fair - not a lot but, you know, he buys,
1112		like, a few hundred a week. You know and he's...
1113		
1114	A:	All right.
1115		
1116	A5:	...regular.
1117		
1118	A:	Yeah.
1119		
1120	A5:	You know I mean - and then the other day he hands me 600 bucks or 500 and change
1121		and - but then there was 80 one dollar bills man. And I'm like dude.
1122		

A: Yeah. Right.

A5: You wanna give me one dollar bills?

A: Yeah you work at a strip club?

A5: Well he gets 'em from his girls workin' (unintelligible).

A: Oh. (Unintelligible).

A5: But, you know, I do one dollar bills it's 20% of 'em. I don't mind takin' 'em.

A: Yeah.

A5: 20%.

A: Yeah.

A5: I'm not a fuckin', you know, I'm - I don't wanna deme- you know...

A: Well you gotta deal with it.

A5: Well yeah I mean I use it to, like, I - I went to the - we went out to dinner with my girlfriend and I paid the guy in, like, 40 bucks in ones.

A: Yeah.

A5: Whatever I don't...

A: Come on.

EXHIBIT

I

Havocscope
Global Black Market Information

Prostitution Prices in the United States

in Transnational Crime

The typical price for oral sex charged by street prostitutes in the United States is between $20 to $50. For sexual intercourse, street prostitutes typically charge between $50 to $100.

Most sex acts take up to 10 minutes if performed in the car and up to 25 minutes if performed inside a room.

The typical street prostitute works between 6 to 8 hours a day and between 5 to 6 days a week. During a working day, the street prostitute averages between 3 to 5 clients.

(See more world prostitute prices.)

Source: Michael S. Scott and Kelly Dedel, "Street Prostitution," Second Edition, United States Department of Justice, Office of Community Oriented Policing Services, November 28, 2006.

Previous post: Drug seizures in Iran

Next post: Increase in fines from Foreign Corrupt Practices Act

Havocscope
Global Black Market Information

Prostitution Prices

World prostitution prices posted below and the money paid to prostitutes is quoted in U.S. Dollars. The rates and prices for sex are collected from various reports, such as reports by criminal justice programs and public health programs, as well as news reports on where to find prostitutes . How much the prostitutes charge is often based upon the sex worker being a victim of human trafficking.

All prices of prostitutes and additional information about the global sex trade are available in our ebook, Prostitution: Prices and Statistics of the Global Sex Trade.

Click on the price for the original post and source information.

1. Afghanistan$30 to $60
2. Argentina$50 at brothel, $300 at club
3. Australia$150 for Asian woman, $300 for Caucasian woman
4. Bangladesh$0.60
5. Brazil$5.50 for 13 year old girl
6. Brazil – Brothel (Rio)$60 entry fee at Centaurus
7. Brazil – Vila Mimosa, Rio$20
8. Bulgaria$25
9. Canada – Vancouver$147 on Backpage (User Submitted)
10. China – Beijing$100 to $400
11. China – Dongguan$160
12. China – Hotel Spa$130
13. China – Shanghai$650 to $1,600
14. Colombia$200 with Virgin Girl
15. Costa Rica – Brothel$30 at Brothels (User Submitted)
16. Denmark$150 to $200 per hour (User Submitted)
17. Dubai$81 to $136 in studio flat
18. Egypt$400 for Tourists
19. France – Apartment in Paris$207 per client.
20. France – CannesUp to $40,000 a night
21. GermanyFlat Rate of $65
22. Greece$12 to $19 with HIV Positive Girl
23. Hong Kong$40 in a one-room brothel to $232 in hostess bar

24. Hong Kong – 17 y/o minor$50 to $65
25. India$1,000 for virgin, $1 for adult
26. India – Calcutta Prostitute Earnings$1.85 per day
27. India – Delhi$13.50 to $16.80 for foreign women
28. India – Online$573 for two hours
29. Indonesia – Earnings for Prostitute$784 to $1,120 per month
30. Indonesia – Social Media$70 on Facebook
31. Iran – Tehran$50 to $65 for Street Prostitute
32. Iraq$100 per session / $200 per night
33. Ireland$45 to $129 charged by male prostitutes
34. Ireland -Limerick$107 to $133 online, $40 to $66 street price.
35. Japan$125 for 60 minutes with a South Korean prostitute
36. Japan – Minor$100 for sex with 14-year old
37. Japan – Tokyo$118 at brothels
38. Jordan$1,000 for Filipino Woman
39. Kenya$25 for sex with 12 year old girl
40. Kenya Border$11.25 Kenyan Prostitute, $2.00 Ugandan Prostitute
41. Kurdistan$150
42. Kuwait$700 for 3 hours with escort (User Submitted)
43. Madagascar$15 for one session with 15 year-old girl
44. Maldives$9.77 for children
45. Mali$2
46. Malaysia$100 for sex with child
47. Mexico$50 per hour with street walker(User Submitted)
48. Mexico – Male Prostitutes$40 for 40 minuets
49. Netherlands – Amsterdam$68
50. Nigerian women in Italy$13 per transaction
51. Nigerian women in Ivory Coast$2 per act
52. Philippines – Subic Bay$35 at bars
53. Poland$30 to 50 per hour
54. Scotland – Edinburgh$48
55. Serbia$10 to $500, average $60. (User submitted).
56. Singapore$25,000 for 3-day tour
57. Singapore – Minor$47 to $55
58. Singapore – Online$111 to $119 for 90 minutes
59. South Korea – Jongmyo Park$19 – $29 for Elder Women
60. South Korea – Southern Seoul$117
61. South Korea – Underage Girl$275
62. SurinameOne gram of gold
63. SwitzerlandUnion minimum of $100
64. Syrian Women$7 at refugee camp
65. Taiwan$344 for South Korean Prostitute
66. Turkey$500 for VIP service (User Submitted)
67. Ukraine$124 to $248 for foreign language speaking prostitute
68. United Kingdom – London Male Prostitute$229 per hour
69. United Kingdom – Street Prostitute$20
70. United States$50 to $100 for street prostitute
71. United States – High-End Escort in Indianapolis$500 per hour
72. United States – High-End Escort in NYC$10,000 a night
73. United States – Legal Brothel in Nevada$200 to $600
74. United States – Massage Parlor$200 to $400 for oral sex and intercourse
75. United States – Massage Parlor Worker Earnings$8,000 to $10,000
76. United States – Minnesota$60 for oral sex with minor found on Backpage
77. United States – Oregon (Ashland)$200 to $500 per hour (User Submitted)

78. United States – Oregon (Portland)$130
79. United States – Orlando$300 to $400 per hour
80. United States – Pennsylvania Earnings$20.00 a week
81. United States – Phoenix, AZ$1,500 per day for lesbian escorts
82. United States – Prison Guard$150 charged by female guards
83. United States – Santa Ana, CAUnder $100 per act
84. United States – Silicon Valley$350 to $500 per hour
85. United States – Underage Girls$40 to $100 for 15 to 30 minutes of sex
86. United States – Washington, DC$200 an hour

Additional Prostitution Information:

Prostitution Statistics

Number of Prostitutes in the World

Prostitution Revenue by Country

- **Search Havocscope**

  To search, type and hit enter

- **Folllow Havocscope on Facebook and Twitter to get more news about the black market.**

EXHIBIT

J

Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2013-G001
Issued: March 18, 2013
Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[1] Such persons are referred to in this guidance as "users," "administrators," and "exchangers," all as defined below.[2] A user of virtual currency is ***not*** an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger ***is*** an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

Currency vs. Virtual Currency

FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[3] In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

[1] FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. *See* Treasury Order 180-01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.

[2] FinCEN's regulations define "person" as "an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities." 31 CFR § 1010.100(mm).

[3] 31 CFR § 1010.100(m).

Background

On July 21, 2011, FinCEN published a Final Rule amending definitions and other regulations relating to money services businesses ("MSBs").[4] Among other things, the MSB Rule amends the definitions of dealers in foreign exchange (formerly referred to as "currency dealers and exchangers") and money transmitters. On July 29, 2011, FinCEN published a Final Rule on Definitions and Other Regulations Relating to Prepaid Access (the "Prepaid Access Rule").[5] This guidance explains the regulatory treatment under these definitions of persons engaged in virtual currency transactions.

Definitions of User, Exchanger, and Administrator

This guidance refers to the participants in generic virtual currency arrangements, using the terms "user," "exchanger," and "administrator."[6] A *user* is a person that obtains virtual currency to purchase goods or services.[7] An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

Users of Virtual Currency

A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is ***not*** an MSB under FinCEN's regulations.[8] Such activity, in and of itself, does not fit within the definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.[9]

---

[4] *Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011) (the "MSB Rule"). This defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States." 31 CFR § 1010.100(ff).

[5] *Final Rule – Definitions and Other Regulations Relating to Prepaid Access*, 76 FR 45403 (July 29, 2011),

[6] These terms are used for the exclusive purpose of this regulatory guidance. Depending on the type and combination of a person's activities, one person may be acting in more than one of these capacities.

[7] How a person engages in "obtaining" a virtual currency may be described using any number of other terms, such as "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing," depending on the details of the specific virtual currency model involved. For purposes of this guidance, the label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the BSA of the process or of the person engaging in the process.

[8] As noted above, this should not be interpreted as a statement about the extent to which the user's activities comport with other federal or state statutes, rules, regulations, or orders. For example, the activity may still be subject to abuse in the form of trade-based money laundering or terrorist financing. The activity may follow the same patterns of behavior observed in the "real" economy with respect to the purchase of "real" goods and services, such as systematic over- or under-invoicing or inflated transaction fees or commissions.

[9] 31 CFR § 1010.100(ff)(1-7).

Administrators and Exchangers of Virtual Currency

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason ***is*** a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.[10] FinCEN's regulations define the term "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[11]

The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.[12] FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and de-centralized convertible virtual currencies.

a. E-Currencies and E-Precious Metals

The first type of activity involves electronic trading in e-currencies or e-precious metals.[13] In 2008, FinCEN issued guidance stating that as long as a broker or dealer in real currency or other commodities accepts and transmits funds solely for the purpose of effecting a *bona fide* purchase or sale of the real currency or other commodities for or with a customer, such person is not acting as a money transmitter under the regulations.[14]

However, if the broker or dealer transfers funds between a customer and a third party that is not part of the currency or commodity transaction, such transmission of funds is no longer a fundamental element of the actual transaction necessary to execute the contract for the purchase or sale of the currency or the other commodity. This scenario is, therefore, money

---

[10] FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)–(F).

[11] 31 CFR § 1010.100(ff)(5)(i)(A).

[12] Ibid.

[13] Typically, this involves the broker or dealer electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency. However, the same conclusions would apply in the case of the broker or dealer issuing paper ownership certificates or manifesting customer ownership or control of real currencies or commodities in an account statement or any other form. These conclusions would also apply in the case of a broker or dealer in commodities other than real currencies or precious metals. A broker or dealer of e-currencies or e-precious metals that engages in money transmission could be either an administrator or exchanger depending on its business model.

[14] *Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and other Commodities*, FIN-2008-G008, Sept. 10, 2008. The guidance also notes that the definition of money transmitter excludes any person, such as a futures commission merchant, that is "registered with, and regulated or examined by…the Commodity Futures Trading Commission."

transmission.[15] Examples include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer's account; (2) the transfer of value from a customer's currency or commodity position to the account of another customer; or (3) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party. Since the definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies, the same rules apply to brokers and dealers of e-currency and e-precious metals.

b. Centralized Virtual Currencies

The second type of activity involves a convertible virtual currency that has a centralized repository. The administrator of that repository will be a money transmitter to the extent that it allows transfers of value between persons or from one location to another. This conclusion applies, whether the value is denominated in a real currency or a convertible virtual currency. In addition, any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on behalf of others, including transfers intended to pay a third party for virtual goods and services, is also a money transmitter.

FinCEN understands that the exchanger's activities may take one of two forms. The first form involves an exchanger (acting as a "seller" of the convertible virtual currency) that accepts real currency or its equivalent from a user (the "purchaser") and transmits the value of that real currency to fund the user's convertible virtual currency account with the administrator. Under FinCEN's regulations, sending "value that substitutes for currency" to another person or to another location constitutes money transmission, unless a limitation to or exemption from the definition applies.[16] This circumstance constitutes transmission ***to another location***, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator. It might be argued that the exchanger is entitled to the exemption from the definition of "money transmitter" for persons involved in the sale of goods or the provision of services. Under such an argument, one might assert that the exchanger is merely providing the service of connecting the user to the administrator and that the transmission of value is integral to this service. However, this exemption does not apply when the only services being provided are money transmission services.[17]

The second form involves a *de facto* sale of convertible virtual currency that is not completely transparent. The exchanger accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the exchanger's own convertible virtual currency held with the administrator of the repository. The exchanger then transmits that

[15] In 2011, FinCEN amended the definition of money transmitter. The 2008 guidance, however, was primarily concerned with the core elements of the definition – accepting and transmitting currency or value – and the exemption for acceptance and transmission integral to another transaction not involving money transmission. The 2011 amendments have not materially changed these aspects of the definition.
[16] See footnote 11 and adjacent text.
[17] 31 CFR § 1010.100(ff)(5)(ii)(F).

internally credited value to third parties at the user's direction. This constitutes transmission ***to another person***, namely each third party to which transmissions are made at the user's direction. To the extent that the convertible virtual currency is generally understood as a substitute for real currencies, transmitting the convertible virtual currency at the direction and for the benefit of the user constitutes money transmission on the part of the exchanger.

c. De-Centralized Virtual Currencies

A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort.

A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.

Providers and Sellers of Prepaid Access

A person's acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies.[18]

Dealers in Foreign Exchange

A person must exchange the currency of two or more countries to be considered a dealer in foreign exchange.[19] Virtual currency does not meet the criteria to be considered "currency" under the BSA, because it is not legal tender. Therefore, a person who accepts real currency in

[18] This is true even if the person holds the value accepted for a period of time before transmitting some or all of that value at the direction of the person from whom the value was originally accepted. FinCEN's regulations define "prepaid access" as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number." 31 CFR § 1010.100(ww). Thus, "prepaid access" under FinCEN's regulations is limited to "access to funds or the value of funds." If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency." 31 CFR § 1010.100(ff)(5)(i) .

[19] FinCEN defines a "dealer in foreign exchange" as a "person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery." 31 CFR § 1010.100(ff)(1).

exchange for virtual currency, or *vice versa*, is not a dealer in foreign exchange under FinCEN's regulations.

* * * * *

Financial institutions with questions about this guidance or other matters related to compliance with the implementing regulations of the BSA may contact FinCEN's Regulatory Helpline at (800) 949-2732.

EXHIBIT

K

32.1.1.2.6 (09-23-2011)

Interpretative Regulations

The Administrative Procedure Act (APA) exempts interpretative rules from the APA's notice and comment requirements. Generally, rules or statements issued by an agency to advise the public of the agency's construction of the statutes it administers are considered interpretative. Most IRS/Treasury regulations are considered interpretative because the underlying statute implemented by the regulation contains the necessary legal authority for the action taken and any effect of the regulation flows directly from that statute. See CCDM 32.1.1.2.7 and CCDM 32.1.1.2.8, below, and CCDM 32.1.5.4.7.5.1(2), Administrative Procedure Act, for further discussion on whether a regulation is interpretive or legislative.

Internal Revenue Manual, available at https://www.irs.gov/irm (last accessed October 10, 2017).