EXHIBIT B

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Maryland

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

Premises at [redacted] Lillian Lane, Laurel, MD 20723 and the persons of Shaun Bridges & Ariana Esposito

Case No. 16-0197TJS

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Maryland, Baltimore Division
(identify the person or describe the property to be searched and give its location):

See Attachment A2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B2

YOU ARE COMMANDED to execute this warrant on or before February 6, 2016 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Timothy J. Sullivan, Magistrate Judge or duty USMJ.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☑ for 10 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: January 27, 2016 4:19 pm

Judge's signature

City and state: Baltimore, MD

Timothy J. Sullivan, Magistrate Judge
Printed name and title

16-0197TJS

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Maryland

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* SEARCH OF INFORMATION ASSOCIATED WITH BRANSTEIN.GUSTAF@OUTLOOK.COM STORED AT PREMISES CONTROLLED BY MICROSOFT	)	Case No. 16-0198TJS

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A" (Property to be Searched) (attached hereto and incorporated by reference)

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

Items as described in Attachment B, attached hereto.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 6, 2016 *(not to exceed 10 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Duty magistrate Judge *(name)*.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: January 27, 2016 4:18pm

Judge's signature

City and state: Baltimore, MD

Honorable Timothy J. Sullivan

Printed name and title

16-0198TJS

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maryland

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

SEARCH OF INFORMATION ASSOCIATED WITH BRANSTEIN.GUSTAF@OUTLOOK.COM STORED AT PREMISES CONTROLLED BY MICROSOFT

Case No. **16-0198TJS**

APPLICATION FOR A SEARCH WARRANT

I, 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)*:

See Attachment "A" (Property to be Searched) (attached hereto and incorporated by reference)

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

Items as described in Attachment B, attached hereto.

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 U.S.C. § 641	theft of government property
18 U.S.C. § 1956	money laundering
18 U.S.C § 1343	wire fraud

The application is based on these facts:

See attached Affidavit of S/A T Gambaryan.

Approved as to form: Richard B. Evans
AUSA HAUN, PIN ATTY EVANS

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days (give exact ending date if more than 30 days: 05/31/2016) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

IRS SPECIAL AGENT TIGRAN GAMBARYAN
Printed name and title

Sworn to before me and signed in my presence.

Date: January 27, 2016

Judge's signature

City and state: Baltimore, MD

Honorable Timothy J. Sullivan
Printed name and title

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maryland

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

The premises located at [redacted]1 Lillian Lane, Laurel, MD 20723 and the persons of Shaun Bridges and Ariana Esposito

Case No. 16-0197TJS

APPLICATION FOR A SEARCH WARRANT

I, 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)*:

See Attachment A2 to Affiidavit in Support of Search Warrant

located in the _____ District of Maryland, Baltimore Division, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B2 to Affidavit in Support of Search Warrant

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 U.S.C. § 641	Theft of Government Property
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. §§ 1956 & 922(g)	Money Laundering, Firearms Violations

The application is based on these facts:

See Affidavit in Support of Search Warrant

- ☐ Continued on the attached sheet.
- ☑ Delayed notice of 10 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.

Applicant's signature

Tigran Gambaryan, Special Agent, IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date: January 27, 2016

Judge's signature

City and state: Baltimore, MD

Timothy J. Sullivan, Magistrate Judge
Printed name and title

16-0197TJS

16-0198TJS

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

I, Tigran Gambaryan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service (IRS-CI) in the Northern District of California and have been since 2011. I am currently detailed to the IRS Cyber Crimes Unit (IRS-CI CCU) and the National Cyber Investigative Joint Task Force (NCIJTF) in Washington, D.C. Prior to my IRS-CI employment, I was as an auditor for California's Franchise Tax Board, where I investigated abusive tax shelters. My training and experience includes, but is not limited to, investigations involving money laundering, white collar fraud, public corruption, organized crime, and violations of the Bank Secrecy Act and tax code. I have developed a specialty in cyber and digital currency crimes.

2. I am "an investigative or law enforcement officer" of the United States within the meaning of Title 18, United State Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, violations of federal law.

3. I make this affidavit in support of two separate warrants for different purposes. First, I submit this affidavit in support of an application for a search warrant for certain records controlled by the electronic communications service provider Microsoft Corporation (Microsoft) headquartered at One Microsoft Way, Redmond, WA 98052-6399, relating to the email address branstein.gustaf@outlook.com. As set forth herein, there is probable cause to believe that the records and information contained in this email account, further described in Attachment A, contain evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C § 1343

(wire fraud); 18 U.S.C. § 1956 (money laundering); and/or 18 U.S.C. § 641 (theft of government property), as further described in Attachment B. Second, this affidavit is also submitted in support of an application for a search warrant for the residence of former Secret Service Agent Shaun Bridges and his wife, Ariana Esposito, located at [redacted] Lillian Lane, in Laurel, Maryland, hereinafter "PREMISES" as well as any electronic devices or evidence found in the PREMISES and/or on the persons of Bridges and/or Esposito. As set forth herein, there is probable cause to believe that the locations further described in Attachment A2 contain evidence, instrumentalities, contraband and/or fruits of the same violations identified above in this paragraph, and further described in Attachment B2 as well as violation of 18 U.S.C. § 922(g) (firearms violations).

4. The facts and information contained in this affidavit are based on my personal knowledge, as well as observations of other law enforcement officials involved in this investigation. All observations that were not personally made by me were related to me by the persons who made them or by representatives of those persons. This affidavit does not contain each and every fact known to the government but only those necessary to support a finding of probable cause.

5. I have set forth facts that I consider are sufficient to establish probable cause to believe that the locations described in Attachments A and A2 will contain evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1343 (Wire Fraud), 641 (Theft of Government Funds), 1956 (Money Laundering), and/or 18 U.S.C. § 922(g) (Firearms Violations). This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

JURISDICTION

6. This affidavit is made in support of an application for a search warrant pursuant to 18 U.S.C. § 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the United States records and other information pertaining to the subscriber(s) and/or customer(s) associated with the email account branstein.gustaf@outlook.com, including the contents of communications.

7. This court has jurisdiction to issue the requested warrant seeking records and information from Microsoft because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Under Section 2711(3)(A)(i), a court of competent jurisdiction is "a district court of the United States that has jurisdiction over the offense being investigated."[1] As discussed below, although former Secret Service Agent Shaun Bridges was prosecuted and sentenced in the Northern District of California for obstruction of justice and money laundering stemming from his theft of bitcoins during the course of his participation in a federal criminal investigation, there is a new investigation into additional, and as of yet uncharged, criminal conduct for which jurisdiction may lie in either the District of Maryland and the Northern District of California, and agents on both coasts are working on the instant investigation.

8. This affidavit is also made in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to search the PREMISES and the persons of Shaun Bridges

[1] For these reasons a court in the Northern District of California would also be a court of competent jurisdiction from which to seek a warrant for the electronic records. In my training and experience there is often more than one district that contains a court of competent jurisdiction. In this case given that a search warrant is being sought for physical premises and items physically located in the District of Maryland, I seek the warrant for the electronic records out of Maryland in the interests of a conservation of judicial and investigative resources.

and his wife, Ariana Esposito for evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. § 922(g) (firearms violations), and/or 18 U.S.C § 1343 (wire fraud); 18 U.S.C. § 1956 (money laundering); and/or 18 U.S.C. § 641 (theft of government property) on things such as cellular telephones, thumb drives, etc., as further described in Attachment B2. Since the PREMISES are located in Maryland, as are the persons of Bridges and Esposito, the District of Maryland has jurisdiction to issue a search warrant authorizing the requested search warrant.

BITCOIN BACKGROUND

9. Bitcoin is a form of decentralized convertible virtual currency that exists through the use of an online decentralized ledger system. While Bitcoin mainly exists as an internet-based form of currency, it is possible to "print out" the necessary information and exchange Bitcoin via physical medium. The currency is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire bitcoins, a typical user will purchase them from a Bitcoin seller or "exchanger." It is also possible to "mine" bitcoin by verifying other users' transactions. Bitcoin is just one form of digital currency; there are a significant number of other varieties of digital currency.

10. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value from government regulation or law), or other convertible virtual currencies in order to obtain bitcoins. When a user wishes to purchase bitcoins from an exchanger, the user will typically send payment in the form of fiat or other convertible virtual currency to an exchanger, usually via wire or ACH, for the corresponding number of bitcoins based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase

with another user of the exchange that is trying to sell bitcoins, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed.

11. When a user acquires bitcoins, the bitcoins are sent to the user's Bitcoin address. This is somewhat analogous to a bank account number, which is comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can then conduct transactions with other Bitcoin users, by transferring bitcoins to their Bitcoin addresses, via the internet.

12. Little to no personally identifiable information about the payer or payee is transmitted in a Bitcoin transaction. Bitcoin transactions occur using a public key and a private key. A public key is used to receive bitcoins and a private key is used to allow withdrawals from a Bitcoin address. Only the Bitcoin address of the receiving party and the sender's private key are needed to complete the transaction, which by themselves rarely reflect any identifying information.

13. All Bitcoin transactions are recorded on what is known as the block chain. Block chain is essentially a distributed public ledger that keeps track of all Bitcoin transactions, incoming and outgoing, and updates approximately six times per hour. The block chain records every Bitcoin address that has ever received a bitcoin and maintains records of every transaction and all the known balances for each Bitcoin address.

14. Digital currencies, including Bitcoin, have many known legitimate uses. However, much like cash, bitcoins can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move money anonymously. As is demonstrated herein, however, in some circumstances bitcoin payments may be traced to accounts at traditional financial institutions using the block chain.

SAN FRANCISCO PROSECTION OF CORRUPT FEDERAL AGENTS

15. Beginning in 2012, the government had multiple investigations into the Silk Road marketplace, an underground black market that allowed vendors and buyers to conduct illegal transactions over the internet. One of these investigations was conducted in the Southern District of New York (SDNY); the other investigation was conducted out of Baltimore in the District of Maryland. Shaun Bridges, former Special Agent for the U.S. Secret Service (USSS) Baltimore Field Office, and Carl Force, former Special Agent for the DEA Baltimore field officer, were assigned to the Baltimore investigation and were not part of the New York investigation. The New York and Baltimore investigations were conducted independently of each other.

16. In 2012, Bridges was assigned to and had significant responsibilities related to the Baltimore Division's Silk Road investigation. In this capacity, Bridges was the computer forensics and technical expert on the Baltimore Silk Road Task Force. In his capacity as a member of the Baltimore Silk Road Task Force, Bridges had significant exposure to and developed expertise in the digital currency known as Bitcoin. My investigation has also revealed that he developed expertise in anonymizing tools such as TOR (The Onion Router) and mixers and tumblers, to be discussed later in this affidavit.

17. In 2012, former DEA Special Agent Carl Force also had significant responsibilities related to the Baltimore Division's Silk Road investigation. In fact, Force was the lead undercover federal agent in communication with Ross Ulbricht, who was later convicted in the SDNY of running the Silk Road.

18. Bridges and Force abused their positions as federal agents and engaged in a scheme to defraud a variety of third-parties, the public, and the government, for their own financial enrichment. On or about March 17, 2015, then-Special Agent Bridges became the target of a criminal investigation in the Northern District of California in connection with the Silk Road investigation. He was placed on administrative leave and then resigned the following day—March 18. On March 25, 2015, Bridges was charged with wire fraud and money laundering stemming from his theft of bitcoins from the Silk Road investigation by the United States Attorney's Office for the Northern District of California (NDCA). On June 15, 2015, Bridges signed an agreement to plead guilty to money laundering and obstruction of justice in the U.S. District Court for the NDCA. On August 1, 2015, Bridges pleaded guilty to money laundering and obstruction of justice. On December 7, 2015, Bridges was sentenced to 71 months incarceration; three years supervised release, and $1,127,275.80 in forfeiture and restitution. Bridges has been out of custody on court-ordered conditions of release since March 2015. The government has moved for his remand at his plea and sentencing. Bridges is scheduled to self-surrender at FCI Berlin on January 29, 2016.

19. Like Bridges, Force also abused his position as a federal agent in a wide variety of ways for his own financial enrichment. Force was also a target of a federal investigation in the Northern District of California in connection with the Silk Road investigation. Like Bridges, Force was charged with federal offenses, including extortion, money laundering and wire fraud, in the NDCA. On July 1, 2015, Force pleaded guilty to these offenses in the NDCA and was sentenced in October 2015 to a term of imprisonment of 78 months, a term of supervised release, and restitution and forfeiture. Unlike Bridges, Force has been in continuous federal custody since his arrest in Spring 2015.

NOVEMBER 2014 BITSTAMP SEIZURE

20. The initial focus of the NDCA corruption investigation regarding the Baltimore Silk Road Task Force was Carl Force. By May 2014, the NDCA investigative and prosecutorial team was aware that Force had approximately $200,000 worth of bitcoins sitting in an account at Bitstamp, a digital currency exchange based in Slovenia and the UK. Given the ongoing NDCA criminal investigation, the government and Force (through his attorneys) entered a written agreement to permit Bitstamp to freeze Force's bitcoins pending resolution of the government's investigation of Force. Bitstamp did so. The expectation was that in the event the NDCA case proved those funds were tied to criminal conduct by Force and represented criminal proceeds, the government would move to have them seized and forfeited.

21. No later than summer of 2014, Bridges was aware of the government's investigation into Carl Force.

22. In November 2014, the U.S. Attorney's Office for the District of Maryland, working with then-Special Agent Bridges and with another member of the Baltimore Silk Road Task Force, sought and obtained a seizure warrant out of the District of Maryland for following property at Bitstamp (hereinafter the "November Bitstamp warrant"): (1) cash; (2) funds in a bank account; and (3) 1606.6488 bitcoins from various Bitstamp accounts. The affidavit in support of the warrant claimed that certain Bitstamp account owners did not supply basic account holder information by identifying their name, address, phone number and instead only supplied email addresses. Bridges was the affiant on the warrant and executed it against Bitstamp on or about November 18, 2014.

23. At the time of the execution of the seizure warrant, the bitcoins at issue in the November Bitstamp warrant alone were worth approximately $600,000. This figure represents

the value on November 18, 2014 when the bitcoin rate was approximately $372.377 U.S. Dollars per bitcoin multiplied by 1606.6497.

24. Among the Bitstamp customers' accounts that were seized pursuant to the warrant was the account of former DEA agent Carl Force which contained approximately $200,000 worth of bitcoins, the same funds that the NDCA and Force's defense attorneys had agreed in writing would be frozen by Bitstamp pending the outcome of the NDCA criminal investigation. Although there were approximately 5072 Bitstamp email addresses associated with accounts that were the subject of the seizure warrant, most of those accounts contained very nominal amounts, and funds in Force's Bitstamp account represented by far the largest portion of funds at issue in the November Bitstamp warrant and approximately twenty five percent of the total amount of bitcoin seized.

25. On approximately December 3, 2014, Bitstamp complied with the November Bitstamp seizure warrant and sent the bitcoins to the bitcoin address 1AUEVwmGLCkpEWAuh XhZnP7NcecDbr5jj9 (hereafter referred to as the "5jj9" wallet), which based on my understanding of the bitcoin protocol was a wallet created by Bridges as the affiant on the warrant. This digital wallet created to hold the forfeited funds contains the wallet address or identification (ending in 5jj9) and a discreet privacy key, which was established to protect the newly created wallet from theft or intrusion. In order to transfer bitcoins out of the wallet the private key is required. Bridges saved this information, containing the wallet identification and private key, associated with the Bitstamp digital wallet to a compact disc (CD). It was determined through interviews of USSS personnel that Bridges was the only Baltimore USSS Agent that had the expertise to create the private key for the seizure wallet. Additionally, a review of USSS evidence inventory documents show that Bridges secured the CD containing the private key on December 2, 2014. No other USSS personnel is listed on the inventory documents as accessing the CD from the time Bridges placed it into the evidence vault until the time certain thefts occurred and were discovered in December 2015 (described further below). Once saved to a CD, Bridges entered it into evidence and secured in the USSS Baltimore Field Office evidence vault. However, based on my training

and experience in digital currency cases I know that even though this CD was logged into evidence, Bridges could have made duplicate CDs containing the private key data required to transfer the bitcoins out of the Bitstamp wallet. Importantly, no one at Bitstamp would have had the private key needed to transfer the bitcoin out of the wallet.

26. Meanwhile, upon being served with the November Bitstamp warrant, Bitstamp contacted the prosecutors and agents in NDCA case and apprised them of the District of Maryland's seizure warrant, a seizure warrant which had not been shared with the government prosecutors or agents in NDCA or known to the NDCA investigative team.

27. By Fall 2015, various Bitstamp account owners whose accounts were the subject of the November Bitstamp warrant disputed the legality of that warrant. Subsequently, pursuant to a court order dated September 11, 2105 (Case No. 14-2651.SAG), in the U.S. District Court for the District of Maryland, the USSS was directed to return 125.38885781 bitcoins (worth approximately $30,616.69 at the time of the order) to Bitstamp for reimbursement to the affected Bitstamp clients. Separately, as part of his plea agreement, Force agreed to administratively forfeit the approximately $200,000 of the seizure that represented his Bitstamp account.

BRIDGES HAD ACCESS TO THE BITCOINS SEIZED PURSUANT TO THE NOVEMBER BITSTAMP WARRANT AFTER HE RESIGNED AND WAS CHARGED WITH CRIMES

28. The NDCA's corruption investigation initially focused on Carl Force. However, due to certain facts and the government's analysis of the blockchain for various bitcoin transactions at issue in that case, the NDCA investigation ultimately expanded to include other(s) on the Baltimore Silk Road task force, including Bridges.

29. In fact, by late March 2015 Bridges was charged with a variety of crimes alongside Force, including obstruction, money laundering and wire fraud. In sum, Bridges pleaded guilty to having used a cooperating witness' login and password credentials to access various Silk Road vendors' accounts and transfer bitcoins out of those wallets and into a wallet that he controlled.

Ultimately, Bridges liquidated those funds into U.S. dollars into a personal account that he controlled. In other words, Bridges stole the funds out of the various vendors' accounts, made it appear as if the cooperating witness had done so, and then transferred them to an offshore digital currency exchange in Japan, Mt. Gox. Between March and May 2013, those funds were liquidated from Mt. Gox to an account Bridges had set up with Fidelity in the U.S. in the name of Quantum LLC, a shell company Bridges had established for the purpose of effectuating his fraud. Two days after his last withdrawal from Mt. Gox, Bridges actually served as the affiant on a separate seizure warrant directed at Mt. Gox.

30. Initially, Bridges indicated a desire to self-surrender and to cooperate with the government in its investigation into the Silk Road Task Force. However, Bridges was untruthful in his early interactions with the NDCA investigators and prosecutors, and, as a result, he unusable as a cooperator. Therefore, in April 2015 the government and Bridges' lawyer set about plea discussions and a plea was finalized in or about late June 2015.

31. Meanwhile, on or about April 8, 2015, the Asset Forfeiture Branch of the U.S. Secret Service (USSS) contacted the NDCA team and alerted them that former-Special Agent Bridges had access to the private key of the wallet associated with the November Bitstamp seizure, namely the wallet ending in "5jj9." NDCA, having had no role in the November seizure warrant and having had no control over the fruits or disposition of that warrant – which at that point was subject to a valid federal court order – was not in a position to "undo" the seizure. However, on April 8, 2015, it advised the USSS Asset Forfeiture Branch of the need to promptly move the funds out of the existing 5jj9 wallet to which Bridges still had access, and into another new wallet to which Bridges did not have access. The USSS confirmed that it would do so.

32. The matter was left to the USSS Baltimore Division and the USSS Asset Forfeiture branch to complete the move from the wallet over which Bridges had access to a new wallet over which he did not have control. Unfortunately, the USSS failed to effectuate this move. Thus, despite that Bridges had been charged in a criminal case for stealing bitcoin and transferring it to

his own personal account and was in the process of negotiating a guilty plea for that conduct, Bridges retained his ability to access yet other funds—the funds at issue in the November Bitstamp seizure.

THEFT OF THE GOVERNMENT FUNDS FROM THE NOVEMBER BITSTAMP WARRANT

33. As stated above, various Bitstamp account owners disputed the legality of the November Bitstamp seizure on which Bridges had served as the affiant. Pursuant to a court order Case No. 14-2651.SAG in the U.S. District Court for the District of Maryland dated September 11, 2015, the USSS was directed to return 125.38885781 bitcoins to Bitstamp for reimbursement to the affected Bitstamp clients. On December 14, 2015, when the USSS attempted to transfer these bitcoins back to Bitstamp, the USSS discovered that the total amount of bitcoins, 1606.6497, in the USSS wallet (ending in '5jj9' and established by Bridges) had been moved without authorization to another wallet with the address of 18ntGvhU1Jc8thPhvkVVH8MwAMTDxNh8D5 (hereinafter "h8D5"). The records reflect that the bitcoins were moved, and thus stolen, on or about July 28, 2015. This theft occurred after Bridges has signed a plea agreement with the government, pleading guilty to the theft of bitcoins.

34. To date, the investigation has revealed that Bridges was the only individual known to have possessed and/or have had access to the private key needed to move the bitcoins that were the subject of the November Bitstamp seizure out of the wallet. Although it is possible that other government employees had such access, at present the only individual that is conclusively known to have access was Bridges. As stated below, approximately one dozen other USSS employees have been interviewed and reported that they did not have such access.

35. The NDCA investigative and prosecutorial team was alerted to this theft on or about December 15, 2015. Based on this information, I conducted a blockchain analysis of the 5jj9 wallet, the recipient address for the funds that Bridges originally seized from Bitstamp pursuant to the November Bitstamp warrant. Based on this analysis, on July 28, 2015, at 2:24 UTS, the entire balance of the 5jj9 wallet, or 1,606.6497 bitcoin, was sent to the h8D5 address. I linked h8D5 to a bitcoin exchange, BTC-e, through tools such as WalletExplorer.com. WalletExplorer.com is a clustering tool that allows for open-sourced search of the bitcoin blockchain. WalletExplorer.com also detects when a bitcoin user deposits or withdraws bitcoins through certain services, such as bitcoin exchanges, bitcoin payment processors, bitcoin mining pools, or dark web underground marketplaces.

36. Whoever established the h8D5 electronic wallet used an account at BTC-e, an unregistered bitcoin exchanger that operates outside the United States. I know based on my training and experience that BTC-e operates without appropriate anti-money laundering and "know your customer" policies of their customers, including customers in the United States, which is why they are one of the exchanges of choice for many engaging in criminal conduct.

37. Based on the blockchain analysis I conducted described in the paragraphs above, on or about December 16, 2015, my co-case agents contacted BTC-e customer support in order to obtain additional information for the user that on or about July 28, 2015 deposited the aforementioned 1,606.6497 bitcoins from the USSS wallet ending in 5jj9 to the BTC-e wallet ending in h8D5.

38. On December 17, 2015, BTC-e emailed records associated with the transfer of 1606.6497 bitcoin from the wallet address ending in 5jj9 to the wallet address ending in h8D5. The records revealed that the BTC-e account in question was established on July 28, 2015 and that

on July 28, 2015 a deposit of 1606.6497 bitcoin was made to the BTC-e Bitcoin exchange. The records further revealed that seventeen (17) withdrawals were thereafter made from and transferred out of the BTC-e account. Each withdrawal from BTC-e was in the amount of 100 bitcoin (currently worth approximately $39,000) except for the last withdrawal made on September 24, 2015, which was for the remaining amount of 6.6497 bitcoin. By September 24, 2015, all 1606.6497 bitcoins were transferred completely out of the BTC-e account.

39. I conducted additional blockchain analysis and learned that the Bitcoin wallet addresses contained in the account records BTC-e provided were then anonymized by using a Bitcoin tumbler. A tumbler, as the name suggests, is used to "tumble" funds by disguising them and making it difficult to track where the bitcoins originated. It is a tool frequently used by money launderers and others engaged in criminal activity. Additionally, the BTC-e logs contained the Internet Protocol (IP) addresses of the unidentified user(s) that connected to BTC-e when a transfer was executed. The IP addresses have also been anonymized, by using a service known as The Onion Router (TOR). Thus, I believe whoever was accessing the BTC-e account was using TOR.

40. Part of the December 17, 2015 response from BTC-e was that the subject BTC-e account was registered to an individual associated with the email address branstein.gustaf@outlook.com. BTC-e records also indicated that BTC-e had verified this email address.

41. The information provided by BTC-e did not contain personal identifiers, but it did confirm that on July 28, 2015, an individual or individuals with access to "5jj9" deposited 1,606.6497 into BTC-e deposit address "h8D5" for the benefit of the user associated with the branstein.gustaf@outlook.com account. I know this because only an individual with private key level access to 5jj9 would be able to move funds from this address. The BTC-e user,

branstein.gustaf@outlook.com, utilized numerous TOR exit node IPs and a transaction history for incoming and outgoing transactions was provided by BTC-e. I analyzed the BTC-e account history associated with branstein.gustaf@outlook.com and determined that between July 28, 2015 and September 29, 2015, the user of this account liquidated this account through a series of withdrawals to the following addresses:

1	#1765195313 -6.6497 BTC Withdrawal BTC to address 1L7brGiiYhj25eJ3sy5Go4qzUU2tVA4acr 24.09.15
2	#1762869539 -100 BTC Withdrawal BTC to address 14TyzvJNBGLWJ1x3PyuDEX1gzYdbqkH2o7 23.09.15
3	#1758659810 -100 BTC Withdrawal BTC to address 1NbjvtZWVMbjq92eLhg4WUEdtiUUr1NNbC 21.09.15
4	#1756545817 -100 BTC Withdrawal BTC to address 1EeASusPG55g4Lz6WD9KHZQkS5ABHoGAUo 20.09.15
5	#1754015944 -100 BTC Withdrawal BTC to address 1EeASusPG55g4Lz6WD9KHZQkS5ABHoGAUo 19.09.15
6	#1751508892 -100 BTC Withdrawal BTC to address 14kUsm7jvHsoQJsATS5xh2D7HQBFXzWeMd 18.09.15
7	#1748989297 -100 BTC Withdrawal BTC to address 173Ayc67zC6ZNFfyzmsktUw4v4anTnDgxi 17.09.15
8	#1746405859 -100 BTC Withdrawal BTC to address 16u866Yqrd5WcH1DVDQt7rLskz2PEhdWe9 16.09.15
9	#1743976434 -100 BTC Withdrawal BTC to address 16u866Yqrd5WcH1DVDQt7rLskz2PEhdWe9 15.09.15
10	#1647541890 -100 BTC Withdrawal BTC to address 1CFdcTqiupjvpxpyVQsaHmhJ1pS1fUsxzT 12.08.15
11	#1644646076 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 11.08.15
12	#1641585943 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 10.08.15
13	#1636258844 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 08.08.15
14	#1627614158 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 06.08.15
15	#1624829195 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 05.08.15
16	#1621659974 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 04.08.15
17	#1618505986 -100 BTC Withdrawal BTC to address 19ZnDHhSo91cGtL2FdAxWiVuR1Go9Erbfe 03.08.15

Based on this information, I utilized additional clustering tools in order to determine whether these transactions were funneled through bitcoin services that would identify the user. I determined that the bitcoins withdrawn from the BTC-e account registered to branstein.gustaf@outlook.com were deposited into a bitcoin tumbling service called SharedCoin. SharedCoin works through a serious of transactions that mix coins with those of other individuals, as well as coins belonging to SharedCoin. This masks where the coins came from or were sent to. SharedCoin works through a serious of transactions (5 to 20), mixing coins with a stream of transactions from other users, as well as internal coins that are held by SharedCoin. Based on the complexity of these transactions,

I worked with an expert in the field of blockchain analysis and determined that at least 438.9714 bitcoins from the original coins that were taken from 5jj9 were eventually deposited into 1Gk8snMx7tiL391963HBpTohTvC7Dcdkhr on December 15, 2015. Note that this was after Bridges had entered his guilty plea and was still out of custody on release conditions. As late as January 11, 2015, these coins were still being actively laundered through SharedCoin.

42. Microsoft, which is responsible for outlook email accounts, was served a Grand Jury subpoena on December 18, 2015, for the subscriber information associated with the branstein.gustaf@outlook.com email address. The email address was the only information contained in the BTC-e records that could readily lead to the identity of the unidentified individual(s) who stole the 1606.6497 bitcoin because BTC-e does not comply with U.S. Treasury Bank Secrecy Act reporting requirements, as legitimate Bitcoin exchanges do. As a result, BTC-e does not require "Know Your Customer (KYC)" data. KYC is the process of a financial institution, bitcoin exchanges in this case, of verifying the identity of its clients, before establishing an account. Since BTC-e does not comply fully with KYC laws and regulations and appears to have required only an email address for verification, no subscriber information was contained in the logs. As a result, the agencies investigating this theft, DHS-OIG, DOJ-OIG, IRS-CI and FBI, wish to obtain the content, if any, contained within the branstein.gustaf@outlook.com email account that resides on Microsoft servers, in order to help to identify the subject(s) that stole the 1606.6497 bitcoins from the USSS on July 28, 2015. As of today's values 1606.6497 bitcoin is worth over $700,000.

43. The information that would help identify the individual(s) associated with the aforementioned email account includes subscriber data, Internet Protocol (IP) addresses, address book entries, sent and received email messages and draft email messages that are saved in the

account, but never transmitted to another email account. Microsoft and other email providers log IP addresses that are used at the time the account was established as well as when the user connects to Microsoft servers to send and receive email messages. As a result, the account may contain IP addresses that were not anonymized by TOR or other anonymity services, unlike the IP addresses associated with the BTC-e records. Furthermore, even if the unidentified individual responsible for the theft of Bitcoin use TOR or other anonymity services to mask their IP address, vulnerabilities in the services could still leak the user's original IP address. Identification of an IP address can sometimes lead to records that can help reveal the identity of the user(s) or location or address where the user(s) was located.

THEFT OF THE GOVERNMENT FUNDS FROM THE CALLAHAN GOVERNMENT SEIZURE

44. In a separate incident, on November 5, 2014, then-Secret Service Agent Bridges administratively seized 50.44 bitcoins, worth approximately $20,000 at the time of the seizure, from Tom and Amanda Callahan of Hurlock, Maryland (the "Callahan seizure"). The Callahan seizure stemmed from a warrant by the Maryland State Police/Dorchester County, Maryland Narcotics Task Force, in which Bridges participated, for the Callahan residence in Hurlock, Maryland. During the execution of that search warrant, 50.44 bitcoins were identified and seized.

45. On November 5, 2014, the proceeds of the Callahan seizure, 50.44 bitcoin, were transferred to wallet address 18Pf8yVQdURiXT2e3vGbpVJ8XXg1bfzfme (hereinafter "zfme"). The transfer to the "zfme" wallet was presumably made by or at the direction of federal law enforcement officers involved in the Callahan seizure, which included Bridges as the digital

currency expert and fellow Baltimore Silk Road Task Force Members; however, it is at this point undocumented in the case files who created the "zfme" wallet.[2]

46. Importantly, there is and was no record of the "zfme" address in seizure files. All that is listed in the original wallets/addresses seized from the Callahans. The following original addresses associated with the seized wallets were listed:

Wallet 10 59647a405d
1. 1ZF1yVVcin6r2R68Vqd2BQHx9pSQ1HhE8
2. 1MCmLsDhyUFbJ1SusdZEefxct7nUmajfcL

Wallet 10 02bec31cb2
3. 15kviER7Ge6Mg2bRzMHzLToUpWdutUd8KH
4. 1G9tQL5yivPbfjo8zbryRc6575w6qm82jh
5. 1GEBaXsoQ1vP7Zgm5zZabKTo9LEvtThKvQ

47. Shortly after the 50.44 bitcoins were seized, the USSS Asset Forfeiture Branch determined that the funds could not be administratively seized. Specifically, on December 8, 2014, the USSS Asset Forfeiture Branch wrote in an email to Bridges that "After discussing [the seizure] with the Office of Chief Counsel, they decided that the particular facts of the case will not allow the Secret Service to proceed with the administrative seizure process. That decision was reached because OCC determined that there was not probable cause for wire fraud or mail fraud violations, Title 18 U.S.C. § 1960 is not one of the core violations that the Secret Service has jurisdiction over, and under Title 18 U.S.C. § 1956, any laundering appears to be predicated on drug offenses. Therefore, without any additional instances of fraud under the Secret Service Administrative

[2] The affidavit in support of the seizure warrant states that Amanda Callahan "voluntarily transferred the contents of the Bitcoin addressed [listed above] to the agents, and those contents presently are held in the custody of the U.S. Secret Service."

Statutes, this seizure could not be pursued administratively. However, it could still be possible to forfeit the property through the AUSA or at the state level."

48. Therefore, on or about December 29, 2014, then-Special Agent Bridges sought a civil seizure warrant from the District of Maryland. It is unclear currently whether he worked with the U.S. Attorney's Office for the District of Maryland to obtain this seizure warrant. A civil seizure warrant for the 50.44 seized from the Callahans was issued by Magistrate Judge Timothy J. Sullivan on December 29, 2014. The warrant listed, in its Attachment A, the following addresses and made no mention of the "zfme" wallet/address but instead contained the following addresses:

Wallet 10 59647a405d
1. 1ZF1yVVcin6r2R68Vqd2BQHx9pSQ1HhE8
2. 1MCmLsDhyUFbJ1SusdZEefxct7nUmajfcL

Wallet 10 02bec31cb2
3. 15kviER7Ge6Mg2bRzMHzLToUpWdutUd8KH
4. 1G9tQL5yivPbfjo8zbryRc6575w6qm82jh
5. 1GEBaXsoQ1vP7Zgm5zZabKTo9LEvtThKvQ

49. Given the December 2015 discovery of the theft of the bitcoins at issue in the November Bitstamp seizure, the USSS recently checked on the status of the bitcoins that were the subject of the Callahan seizure warrant, to wit:

Wallet 10 59647a405d
1. 1ZF1yVVcin6r2R68Vqd2BQHx9pSQ1HhE8
2. 1MCmLsDhyUFbJ1SusdZEefxct7nUmajfcL

Wallet 10 02bec31cb2
3. 15kviER7Ge6Mg2bRzMHzLToUpWdutUd8KH
4. 1G9tQL5yivPbfjo8zbryRc6575w6qm82jh
5. 1GEBaXsoQ1vP7Zgm5zZabKTo9LEvtThKvQ

50. When these addresses were queried on the blockchain, the results showed that all of the funds were transferred on November 5, 2014 to the aforementioned "zfme"

wallet address. This "zfme" address did not engage in any additional activity until September 10, 2015, when the entire balance was zeroed out and transferred to a series of other addresses. It appears as if this, like the November Bitstamp seizure, was the subject of yet another theft.

ADDITIONAL FACTS RELATED TO SHAUN BRIDGES

Bridges' Theft of Silk Road Bitcoins Is Similar to The Newly Discovered Bitstamp Thefts

51. I am currently investigating other seizures, if any, in which Bridges and/or other members of the Baltimore Silk Road Task Force participated in an effort to determine whether any of those funds also have been stolen. It has been reported to me that the November Bitstamp theft and the Callahan theft described above are not the only thefts, and that there may be thefts of other digital currency seizures that happened outside of Maryland. It should be noted that on the dates of the two additional thefts that have been discovered to date, i.e., the July 28, 2015 theft of the funds at issue in the November Bitstamp warrant and, the September 10, 2015 theft of the funds at issue in the Callahan seizure, former DEA Special Agent Carl Force was in custody in San Francisco, California and had no access to a computer. The same is not true of Bridges.

52. As demonstrated above, Shaun Bridges had access to the wallet and private key needed to access the wallet from which the funds at issue in both the November Bitstamp warrant and the Callahan Warrant were stolen. My DHS-OIG counterparts have interviewed approximately one dozen employees of the USSS and, to date, have learned that Bridges was the only individual who had access to the private key that controlled the wallet from which the bitcoins that were the subject of the November warrant were stolen. As stated, to my knowledge, Bridges was the only individual who possessed or had access to the private key needed to move the bitcoins

that were the subject of the November Bitstamp seizure out of the wallet. An investigation into who, if anyone, aside from Bridges, had access to the Callahan seizure wallet is underway.

53. As discussed above, Bridges was charged with wire fraud, obstruction of justice and money laundering in connection with his theft of bitcoins during the course of the Silk Road investigation -- *United States v. Bridges*, 15-CR-319-RS. The facts of the thefts at issue in that case are very similar to the facts at issue in the instant investigation into the new thefts, i.e., (1) bitcoins to which Bridges had access through his position as a law enforcement agent, (2) were stolen, (3) then moved around from one address to another in an apparent effort to conceal and launder;,and (4) offshore exchanges were used. Bridges pleaded guilty to obstruction of justice and money laundering and admitted the following facts as part of his plea agreement:

> On or about January 25, 2013, I devised a scheme to defraud and to obtain money and property through false and fictitious representations. I utilized an administrator account on the Silk Road website belonging to another individual, and not intended for me or my personal use, to obtain access to that site. I am aware and agree that the government could prove that Silk Road was a website where illegal goods were posted for sale, including narcotics, and that payments were accepted on the site in Bitcoin. I used the administrator account to reset passwords of vendor accounts and other accounts to give me access to those accounts and any bitcoin in the accounts. I then moved a total of approximately 20,000 bitcoin from various Silk Road vendor accounts into a "wallet" over which I exercised control. The value at the time the bitcoin was stolen was approximately $350,000. On January 26, 2013, I moved the bitcoin into an account at Mt. Gox, a digital currency exchange based in Japan.
>
> On January 27, 2013, I attempted to lull the manager of the Silk Road site, Ross William Ulbricht, a/k/a "Dread Pirate Roberts," a/k/a "DPR," by telling him that I, too, had had bitcoin stolen from me. This communication took place by interstate wire; I agree that the government could prove that Ulbricht was in the Northern District of California on that date, and that I was in Maryland.
>
> Between March and May of 2013, I converted the bitcoin into U.S. currency and caused wire transfers of money totaling approximately $820,000 from the accounts at Mt. Gox into a Quantum International Investments, LLC, account I controlled at Fidelity. On June 2, 2014, I transferred funds from that Quantum Fidelity account into an account in the joint names of myself and a person known to the parties. Specifically, I conducted the following financial transactions:

Date	Amount	Description of Financial Transaction
3/6/13	$98,511.08	Wire transfer from Mt. Gox to Quantum Fidelity account
3/8/13	$98,968.00	Wire transfer from Mt. Gox to Quantum Fidelity account
3/13/13	$99,968.62	Wire transfer from Mt. Gox to Quantum Fidelity account
3/18/13	$99,968.74	Wire transfer from Mt. Gox to Quantum Fidelity account
3/19/13	$99,968.64	Wire transfer from Mt. Gox to Quantum Fidelity account
4/5/13	$99,968.08	Wire transfer from Mt. Gox to Quantum Fidelity account
4/16/13	$99,969.34	Wire transfer from Mt. Gox to Quantum Fidelity account

4/26/13	$99,969.32	Wire transfer from Mt. Gox to Quantum Fidelity account
5/7/13	$25,559.37	Wire transfer from Mt. Gox to Quantum Fidelity account
6/2/14	$225,000	Wire transfer from Quantum Fidelity account to PNC Bank in joint name

I knew that the funds in each of the above transactions were the proceeds of wire fraud, and I carried out each of those transactions with the intent both to promote my ongoing wire fraud scheme and to conceal and disguise the nature, location, source, ownership, and origin of those illegal proceeds.

During the time that I devised and carried out this fraud and money laundering scheme, I was a Special Agent with the United States Secret Service and a member of the Electronic Crimes Task Force, and the Baltimore Silk Road Task Force – which was actively engaged in investigating Silk Road, its vendors and buyers, and Dread Pirate Roberts, and for which there was an ongoing Grand Jury investigation in the District of Maryland. I agree that the Baltimore Silk Road Grand Jury investigation was an official proceeding. As a United States Secret Service Special Agent, I held a position of public trust and I abused that position. I further agree that my activities obstructed, influenced, and impeded the Baltimore Grand Jury related to its Silk Road investigation as well as its resulting case in the District of Maryland against Ulbricht by, among other things, (1) obstructing and impeding the ability of the investigation to fully utilize a cooperator's access to Silk Road after my fraud, (2) causing the Task Force and the Grand Jury to spend time and effort to investigate the thefts from Silk Road that I committed, (3) creating additional incentive for Ulbricht to attempt to hire someone to kill a cooperator whom Ulbricht suspected of committing thefts I had in fact committed, and (4) obstructing, influencing, and impeding the Grand Jury's investigation into Ulbricht in the District of Maryland. I agree that I acted corruptly in obstructing, influencing, and impeding the Grand Jury's Silk Road investigation.

I agree that by May of 2014, there was also an active San Francisco-based Grand Jury investigation into potential misconduct by Drug Enforcement Administration (DEA) Special Agent Carl M. Force, IV, and that the San Francisco Grand Jury subsequently began to investigate my conduct. I further agree that the San Francisco Grand Jury investigation was an official proceeding.

On May 28, 2014, I was interviewed by a Special Agent with the Federal Bureau of Investigation (FBI) and I intentionally misled that agent. On November 13, 2014, I was interviewed by a Special Agent from the Department of Justice Office of Inspector General and I intentionally misled that agent as well. During January and February of 2015, I consulted with another employee of the United States Secret Service both before and after that employee had an interview on the subject of this investigation with Special Agents from the Department of Homeland Security Office of Inspector General (DHS OIG) and the FBI. I met with that employee before and after the employee's interview and we discussed the subject of the interview and agreed to tell a false consistent story regarding searches conducted on a database controlled by the Financial Crimes Enforcement Network (FinCEN). On April 2, 2015, in the Northern District of California, I also misrepresented certain facts to agents with the FBI, DHS OIG, Department of Justice Office of Inspector General, and Internal Revenue Service Criminal Investigations, with respect to the full scope of the FinCEN database searches.

I understand and agree that each of the interviews and actions described in the preceding paragraph were in connection with the San Francisco Grand Jury investigation. I further agree that by corruptly encouraging another Secret Service employee to tell a false story to federal agents and by lying to federal agents myself, I obstructed, influenced, and impeded the San Francisco-based Grand Jury investigation into my own criminal conduct and that of former DEA Special Agent Carl M. Force, IV.

54. In contrast to the 2013 conduct at issue in 15-cr-319-RS where Bridges knew that he had not covered his tracks well enough, the perpetrator (s) of the thefts in 2015 knew to use

anonymizing sources such as tumblers and TOR so that the blockchain analysis would be of lesser, if any, value.

55. Bridges signed a Plea Agreement with the government to factual basis conduct on June 15, 2015, but due to his attorney's schedule he did not enter his guilty plea before Judge Seeborg in San Francisco until on or about August 31, 2015. Although the government sought Bridges' remand at the change of plea hearing given certain facts, based on learning that morning of the fact he had tried to change his name (described further below), Judge Seeborg allowed Bridges to remain out on pretrial release with conditions, and directed Bridges to cease efforts to change his name.

56. The government sought Bridges' remand thereafter on two additional occasions: first, when it learned that Bridges had tried to report law enforcement credentials as stolen (described further below). The government's motion for remand was ultimately denied but an additional condition that Bridges not access a computer was imposed on or about October 15, 2015. Second, the government also sought remandat the time of sentencing given Bridges' stated mental issues and given that he had been sentenced to a lengthy prison term of 71 months imprisonment. Judge Seeborg denied the government's request to remand Bridges at sentencing and permitted Bridges to remain out of custody, albeit on strict conditions of release. As such, Bridges was not in custody on July 28, 2015, or on September 10, 2015, when the two thefts described above occurred.

57. During Bridges' time as a federal agent, he was a specialist in tumblers and also in the use of TOR and other anonymizing services.

58. The thief(s) of the bitcoins at issue in the November Bitstamp warrant used TOR and a tumbler, presumably to cover their tracks. I am still investigating whether TOR and bitcoin tumblers were used in connection with the theft of the Callahan funds.

59. As stated above, the bitcoins at issue in the November Bitstamp warrant were stolen on or about July 28, 2015; the BTC-e account to which they were moved was established on or about July 28, 2015; and the Microsoft account associated with the BTC-e account, i.e., Gustaf Branstein, was established on or about July 27, 2015.

PayPal Activity

60. Bridges established a PayPal account in 2002. PayPal has recently reported to law enforcement that transactions that PayPal finds suspicious were conducted in 2015 using Bridges' account. Specifically, Bridges' account appears to have engaged in a number of sales, as a merchant, to third parties for computer hardware and computer equipment. At least two credits to Bridges' PayPal account in September 2015, totaling approximately $6,000, were disputed by different third parties to PayPal. In other words, it appears as though third parties complained to their credit card companies and PayPal was forced to rebate the charges. However, when PayPal went to debit the funds from Bridges' PayPal account, that account was empty. PayPal records indicate that Bridges subsequently transferred those funds to the PayPal account belonging to his wife, Ariana Esposito.

61. Investigation to date has also revealed that on or about June 26, 2015, Bridges' PayPal account was used in an apparent attempt to buy a document from a merchant in Germany that sells birth certificate and related documents. Specially, his PayPal account was debited $149 from a merchant called "Germany-Service" with a description of "birth certificate: international form with an apostille." An apostille is a highly recognized official notary. A search of Germany-

Service's website reveals that they specialize in providing birth certificates. The charge was returned on Bridges' PayPal account the next day, June 27, 2015, for reasons that I am investigating. This was approximately one month before the "Gustaf Branstein" account was established at Microsoft, and also approximately one month before the perpetrator of the November Bitstamp warrant funds established a BTC-e account using the email address in the name of "Gustaf Branstein."

Bridges' Odd Behavior On March 18, 2015

62. On March 18, 2015, Bridges was informed that he was being placed on administrative leave for the conduct that led to the charges in *United States v. Bridges 15-CR-319-RS*.[3]

63. On March 18, 2015, Bridges left for lunch carrying a duffle bag that appeared to be filled and weighted down. See Exhibit 1 attached herewith (stills of photographs of CCTV surveillance photos from USSS Baltimore on March 18, 2015). Bridges returned from lunch without the bag. Even though at that time Bridges was not informed of his suspension, given certain communications I am aware of in the case it is possible that Bridges' lawyer informed Bridges that he was under investigation. Additionally, an inspection of Bridges' government vehicle that afternoon did not uncover the aforementioned bag.

64. That same morning of March 18, 2015 another USSS Special Agent observed Bridges at the "undercover" workstation. Bridges was complaining that someone had changed the undercover computer's password, and added that he was trying to access some case files on another side of the computer. The other agent observed that in his training and experience this could

[3] He was apparently already aware by this point that he was under investigation in connection with the conduct that led to 15-CR-319-RS but had not yet been formally placed on administrative leave by the USSS.

indicate that there was a separate partition or storage area on the computer that Bridges was trying to access.

65. In the afternoon of March 18, 2015, after Bridges was informed that he was being placed on administrative leave for the conduct that led to the charges in *United States v. Bridges*, 15-CR-319-RS, Bridges stated that he wanted to take personal items he had in the office home and repeatedly asked other USSS personnel not to follow him around the office while he did this. First, Bridges went to the Electronic Crimes Special Agent Program (ECSAP) Lab and placed personal items into boxes.

66. After gathering personal items from the ECSAP Lab, Bridges asked his supervisor if he could access his Dell laptop computer to copy electronic receipts of personal items he had purchased from internet merchants. However, instead of copying receipts, Bridges began copying a Microsoft Outlook folder entitled "Bitstamp." Upon noticing what Bridges was copying, his supervisor secured the laptop and did not allow Bridges further access.

67. Bridges took a break to speak with his attorney and when he returned from speaking with his attorney Bridges advised USSS that he was resigning effective immediately. After USSS personnel transported Bridges to his mother's residence, Bridges' USSS escort found what looked like two external hard drives while looking through the items Bridges placed in his vehicle. Both drives were marked "Bridges" with one also stating "Evidence drive." The "evidence drive" was actually a hard drive enclosure that was empty and contained no hard drives. It is believed that the hard drives that were contained in the enclosure were already taken by Bridges earlier in the day when Bridges was observed on CCTV security cameras departing with the duffle bag (Exhibit 1), which Bridges never returned with when he arrived back at the USSS field office. As stated above, the Bitstamp private key was stored as evidence in the Baltimore evidence vault, having

been originally provided to the vault by Bridges. I believe that Bridges may have made a backup of the key needed to access the Bitstamp wallet and that these hard drives that were contained in the enclosure marked "Evidence drive" may have contained just that. The hard drives and contents of the duffle bag are believed to be located at the premises to be searched, unless Bridges or one of his associates has hid or destroyed them.

Bridges' Efforts to Change His Name And Seal Such Change From The Public Record

68. On or about June 28, 2015, Bridges petitioned a Maryland state court to have his named changed from "Shaun Wesley Bridges" to "Calogero Esposito." Esposito is his wife's last name. His justification for the change was past incidents of identity theft and an interest in connecting with his self-identified ancestral heritage. Importantly, Bridges' motion also contained a motion/request to shield the information. Bridges' motions were denied and Bridges re-petitioned the Court two additional times, neglecting to mention that he had been arrested and was scheduled to plead guilty to federal charges in connection with his original bitcoin theft in *United States v. Bridges*, 15-cr-319-RS.

69. The government brought this to Judge Seeborg's attention within a day of learning of this information, which happened to coincide with the change of plea date of August 31, 2015. Bridges' proffered explanation was that he was concerned about the U.S. Office of Personnel Management data breach and that was why he was trying to change his name.

70. In my training and experience as a financial crimes investigator, one of the reasons that those convicted of financial crimes try to change their names and/or identities is to procure new identity documents, often to establish new accounts with financial institutions. Such institutions may then be used to liquidate criminal proceeds. Furthermore, from my training and experience, I know that individuals normally maintain records of their financial activity in their

residence, including receipts for expenditures by cash and check, bank records, and other financial documents. Based on my training and experience, as well as my consultations with other Special Agents with whom I work, I am aware that individuals maintain evidence for long periods of time for several reasons. First, to any individual, the evidence may seem innocuous (e.g., financial, credit card and banking documents, travel documents, receipts, client lists, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the individual may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. Third, the individual may operate under the belief that he/she has deleted, hidden, or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert.

FACTS DEMONSTRATING THAT ARIANA ESPOSITO IS WILLING TO HELP BRIDGES CONCEAL HIS CRIMINAL CONDUCT

Esposito's Relationship With Bridges

71. Ariana Esposito was Bridges' girlfriend during the timeframe in which Bridges committed his crimes to which he pleaded guilty in *United States v. Bridges*, 15-cr-319-RS, to wit, theft of bitcoins from an account that did not belong to him and subsequent laundering of those criminal proceeds. At the time of the investigation, she was his girlfriend. The two did then, and continue to, live together.

72. Esposito was also listed as a joint-account holder on the PNC bank account which received $225,000 in criminally derived proceeds.

Other Conduct

73. As stated above, PayPal identified as suspicious certain chargeback activity involving Bridges' PayPal account in September 2015. When it went to recover the funds from Bridges' PayPal account, it learned that Bridges had transferred funds to a PayPal account belonging to Ariana Esposito.

74. At Bridges' sentencing on December 7, 2015, Esposito testified in support of her husband. The bottom line is that Esposito is an individual who has demonstrated that she supports Bridges. They live together. Bridges tried to change his name to her name, i.e. Esposito, during the aforementioned name change. I know from my training and experience that criminals often use their loved ones, including spouses or significant others, to help commit their crimes, and, also to help conceal their crimes. This can be unwitting on the part of the significant other or purposeful and deliberate. I believe that due to Bridges' sophistication with law enforcement techniques and the fact that he knew he was under investigation and would be closely watched, it is likely that he used and/or was assisted by a third party such as Esposito to assist him in covering his tracks with any other criminal activity in which he was engaged, to include the aforementioned theft of the November Bitstamp warrant.

Bridges' Efforts to Transfer Guns to Esposito

75. On April 1, 2015, as part of the court-ordered conditions for his pretrial release in 15-cr-319-RS, Bridges surrendered four firearms to the Department of Homeland Security (DHS), Office of Inspector General (OIG). Bridges stated that the surrender of his weapons was voluntary, that he could still legally possess the weapons and that he intended to find a third party to assume

ownership of the weapons. A DHS-OIG agent provided Bridges a business card with contact information for when a suitable party was located and explained that the weapons would be transported to and secured at a DHS-OIG facility. On May 28, 2015, the NDCA received an email from the law offices of Rosen Bien Galvan & Grunfeld LLP. Attached to the email was a Firearm Bill of Sale showing that Bridges sold the weapons seized by DHS-OIG to his wife, Ariana Esposito on March 29, 2015, for $1. Notably, the bill of sale was dated with a date when Bridges was on a cross-country flight. Bridges never informed DHS-OIG that he had found a third party, Esposito, to assume ownership of the weapons when he surrendered them on April 1, 2015.

76. Local gun records that were recently discovered, however, show that Bridges did not voluntary surrender all firearms and that he may still be in possession of an item under the Gun Control Act (GCA), 18 U.S.C. § 921, to wit, a regulated silencer that he never surrendered to DHS-OIG. Under the GCA, the silencer is defined as a firearm (18 U.S.C. § 921(a) (3)). On or about June 28, 2014, Bridges purchased the GCA regulated silencer (Surefire .308 caliber) from [redacted] of Select Fire Incorporated, [redacted] Holsum Way, Glen Burnie, MD. The silencer was purchased legally and Bridges completed the required Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives paperwork (ATF Form 4473). On the form, Bridges listed his residence (the PREMISES to be searched) as [redacted] Lillian Lane, Laurel, MD.

77. Under 18 U.S.C. § 922(g), which prohibits possession of a firearm or ammunition by a prohibited person, it is illegal for a convicted felon or persons awaiting trial on felony charges to possess a silencer. It is believed that the prohibited silencer is currently located at the Bridges/Esposito residence.

ADDITIONAL PROBABLE CAUSE RELATING TO EMAIL ACCOUNT

78. As described in the preceding paragraphs, there is probable cause to believe that the email account branstein.gustaf@outlook.com was used to steal seized government assets and linked to the BTC-e account where the stolen bitcoins were transferred into. As a result, there is probable cause to believe that the branstein.gustaf@outlook.com contains evidence of wire fraud, and theft of government funds, and money laundering in violation of 18 U.S.C. §§ 641, 1343 and 1956. Information that Microsoft has provided in response to a Grand Jury subpoena indicated that the aforementioned email account was created on or about July 27, 2015, just one day before the BTC-e wallet was established.

79. Based on your affiant's training and experience, I know that individuals who conspire with others to commit wire fraud, launder currency and theft use e-mail in the furtherance of their criminal activity. Here, I know that the individual(s) at a minimum used this email address to establish an account with BTC-e and that the individual(s) established the email address the very day before the BTC-e account was created, and that the email address was used by BTC-e to verify the account holder.

80. On or about December 17, 2015, your affiant sent a preservation request to Microsoft for the branstein.gustaf@outlook.com email account. In general, an email that is sent to or from a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on a Microsoft's servers for a certain period of time. Therefore, I believe that content of messages sent from the branstein.gustaf@outlook.com accounts may still be maintained on Microsoft's servers.

81. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name outlook.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and retrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

82. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often nevertheless provides clues to their identity, location, or illicit activities.

83. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*,

session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

84. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

85. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each offense-element, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email

communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

ADDITIONAL PROBABLE CAUSE RELATING TO PREMISES, PERSONS, AND DEVICES

86. As stated above, both Bridges' and Esposito's PayPal accounts have been active in the period of time to include the summer and fall of 2015, times during which the thefts that I am now investigating occurred.

87. I know from my training and experience that PayPal accounts are accessed with electronic devices that connect to the internet, such as cellular telephones, computers, and/or ipads.

Therefore, there is probable cause to believe that Bridges and/or Esposito have in their possession an electronic device or devices that may be used to connect to the internet.

88. I further know that on or about June 26, 2015, as stated above, Bridges' PayPal account showed evidence that Bridges had attempted to order a birth certificate from Germany-Service. Again, this was something that was done online. I know in my training and experience that individuals often keep electronic devices in their residence and/or on their persons, depending on the size of the device. This is particularly true for cellular telephones which are effectively computers. It is also true of small storage devices such as a thumb drive.

89. The crimes that are the focus of the instant investigation, i.e., those enumerated in Attachments B and B2, are crimes that in my training and experience are often committed online. I know from my training and experience that individuals who commit crimes online often do so using computer and other electronic devices, in the privacy of their own homes. This is especially true where, as here, Bridges is not permitted to leave his residence under the terms of his court-ordered supervision in 15-cr-319-RS. In addition, I am aware that Esposito is no longer employed by the Maryland State Troopers or in training at their academy and I am aware of no other employment. There is therefore probable cause to believe that such electronic device(s) will be found in the PREMISES or on Bridges' or Esposito's person.

90. In this case that is especially true as Bridges does not have a place of employment, indeed, if he is following newly added court-ordered conditions of release by Magistrate Judge James on October 15, 2015, he is on lockdown at his home with a curfew. Thus, this is not a case where the instrumentalities and/or evidence should be found, for example, on a computer at a public library or at a workplace. Personnel with the Pretrial Services Department advises that Bridges' location monitoring shows he has been at his residence.

91. As described above and in Attachment B2, this application seeks permission to search for records, electronic or otherwise, that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is, but is not limited to, 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).

92. I submit that if a computer, phone, electronic device, or storage medium of any kind is found on the PREMISES, there is probable cause to believe those records will be stored on that device, computer or storage medium, for at least the following reasons:

93. 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.

94. 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.

95. 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.

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

97. Based on actual inspection of other evidence related to this investigation, including but not limited to spreadsheets, financial records, and invoices, I am aware that computer equipment was used to generate, store, and print documents used in the theft, money laundering and wire scheme that I am investigating. There is reason to believe that there is a computer system, in some form, is currently located on the PREMISES.

98. As further described in Attachment B2, 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 reason cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

99. 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, although this information can later be falsified.

100. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contains information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence

relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

101. 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.

102. 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.

103. 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.

104. I know that when an individual uses a computer to obtain unauthorized access to another users' account over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

105. 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:

106. 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.

107. 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.

108. 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.

109. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review 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.

110. Because Bridges shares the PREMISES as a residence with Ariana Esposito, his wife, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons other than Bridges, or jointly owned. In addition for the reasons contained herein, it is believed that Esposito is at a minimum aware of her husband's recent criminal activity, if not outwardly, serving as an accomplice of those crimes or an accomplice after the fact. Thus, if it is possible that the things described in this warrant could be found on any of those computers, devices, or storage media, the warrant applied for would permit the seizure and review of those items as well and they are included in Attachment B2.

CONCLUSION

111. Based on the foregoing, I request that the court issue the proposed search warrants. I believe that the facts described in the preceding paragraphs establish probable cause to believe that there exists on the computer systems controlled by Microsoft, in the PREMISES, and on Bridges and Esposito's persons, that there exists evidence of violations of 18 U.S.C. §§ 1343 (Wire Fraud), 641 (Theft of Government Funds), 1956 (Money Laundering) and 922(g) (Firearms Violations).

16-0197TJS

16-0198TJS

REQUEST FOR SEALING

112. I further request that all papers in support of these application, including the affidavit and search warrants, be sealed until further order of the respective Court. These documents discuss an ongoing criminal investigation, the details of which are neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation. It should be noted that an affidavit containing many of the foregoing details has been provided to Judge Seeborg under seal and ex parte in support of the government's opposition to terminate electronic monitoring for Shaun Bridges.

Respectfully submitted,

Tigran Gambaryan, Special Agent
IRS CI Cyber Crimes Unit

Subscribed and sworn to before me on

January 27, 2016

HONORABLE TIMOTHY J. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

16-0198TJS

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with the email account branstein.gustaf@outlook.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, which is headquartered at One Microsoft Way, Redmond, WA 98052-6399.

16-0198TJS

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Microsoft, Inc. (the "Provider") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 6, 2015, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, from the date of the account's creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

16-0198TJS

d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or email to: Special Agent Todd McHale, Department of Homeland Security-OIG, 45 Hardy Court, Suite 224, Gulfport, MS 39507, email: Todd.McHale@oig.dhs.gov.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1343 (Wire Fraud), 641 (Theft of Government Funds) and 1956 (Money Laundering), and those violations involving the unidentified individual, and/or any additional co-conspirators, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Communications and records related to the theft, trade, transfer and sale of Bitcoin and any financial accounts at any type of financial institution or currency exchange;

2. Information relating to who created, used, or communicated with the email account, including records about their identities and whereabouts;

3. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

8. Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;

9. The identity of the person(s) who created or used the user ID for the email account, including records that help reveal the whereabouts of such person(s); and

10. Identification of co-conspirators, accomplices, and aiders and abettors in the commission of the above offenses.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized

specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States. Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

16-0197TJS

ATTACHMENT A2

Premises and Persons to Be Searched

The premises known as [redacted] Lillian Lane, Laurel, MD 20723 is a residential detached single family home. The street/house number is prominently displayed in black numbers below the mailbox on a wood post at the foot of the driveway. The dwelling is a two story colonial house, with multi-color (brown, tan and gray) stone and tan siding, a single wood with a natural finish front door, there are vertical side windows on each side of the front door, black lamps with clear class are on both sides of the front door, over the front door is a small awning with a black metal roof, slate gray asphalt shingle roof on the rest of the house, five windows on the front of the house, all with white trim and no shutters. The concrete front walk way turns toward the garage side and ends at the asphalt driveway. There is an attached two car garage on the south facing side (left side if facing the front of the house) of the house. The east facing outside wall of the garage is made of stone and has four windows with white trim. The garage door is white with white trim and it is surrounded by siding. To the side and above the garage door are five windows, one on the first story and four on the second story all with white trim on siding. The north facing side of the house (Right-side) is made of siding and has one small window on the first floor, one on the second floor and one on the wall of the exposed basement, all windows have white trim. The basement appears to be made of poured concrete. The electric and gas meters are also on the north facing side (right-side) of the house. In the back of the house there are six windows on the second story, six on the first story and two on the exposed basement. There are sliding doors on the first story and exposed basement, in the back of the house. It is the first house on the left-hand (East) side as you enter and travel north on the Lillian Lane cul-de-sac. Additionally, the front of the premise faces and is across the street from a house with a

red brick front. Your affiant knows Shaun BRIDGES is the owner through Maryland MVA records and the Maryland Department of Assessment and Taxes property records. Additionally in the driveway of the premise there was a red 2002 Toyota Takoma with Maryland tags 39L118. MVA vehicle registration records confirm that Shaun Wesley BRIDGES is the registered owner.

As further stated in the affidavit and Attachment B2, the premises to be searched also includes the persons of Shaun Bridges and Ariana Esposito to locate any of the material enumerated in B2.

16-0197TJS

ATTACHMENT B2

Particular Things to be Seized

All documents, records, and property (whether in the form of printed documents or stored in electronic or digital form on any storage device) that constitute evidence or fruits of 18 U.S.C. § 641 (Theft of Government Property), and/or 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and/or 18 U.S.C. § 922(g) (Firearms Violations) involving SHAUN BRIDGES and others on the Baltimore Silk Road Task Force, including but not limited to the following items:

1. Any information related to Bitcoin thefts or other financial thefts;
2. All computers, iPads hard drives, or other electronic storage media or devices;
3. All bank records, checks, credit card bills, federal and state tax returns, account information, or other financial records;
4. Items belonging to or originating from the U.S. Department of Homeland Security (DHS), and other governmental agencies and departments;
5. Cell phones, PDAs, and other communication devices capable of sending and receiving text messages and online communications;
6. Currency in the form of any denomination to include but not limited to, digital currency, printed money, coins, checks, money orders, etc. in any form; and
7. Stolen government property to include the following:
    a. records in paper and electronic form,
    b. computers and computer equipment,
    c. Law enforcement equipment.
8. Firearms, ammunition, and/or silencers.

16-0197TJS
16-0198TJS

EXHIBIT 1