




**1:15-mj-00656-TJS All Defendants USA v. Force**  
**Date filed: 03/30/2015**  
**Date of last filing: 03/30/2015**

## History

<b>Doc. No.</b>	<b>Dates</b>	<b>Description</b>
<a href="#">1</a>	<i>Filed:</i> 03/30/2015 <i>Entered:</i> 03/31/2015	 Rule 5(c)(3) Documents Received
<a href="#">2</a>	<i>Filed:</i> 03/30/2015 <i>Entered:</i> 03/31/2015	 Initial Appearance - Rule 5(c)(3)
<a href="#">4</a>	<i>Filed:</i> 03/30/2015 <i>Entered:</i> 03/31/2015	 Order of Detention

**Full docket text for document 1:**

Rule 5(c)(3) Documents Received from Northern District of California as to Carl Mark Force (Attachments: # (1) Affidavit)(jks, Deputy Clerk)

**Full docket text for document 2:**

Initial Appearance in Rule 5(c)(3) Proceedings as to Carl Mark Force held on 3/30/2015 before Magistrate Judge Timothy J. Sullivan. (FTR Klein -7B.) (jks, Deputy Clerk)

You do not have permission to view this document.

**Full docket text for document 4:**

ORDER OF TEMPORARY DETENTION as to Carl Mark Force Detention Hearing set for 4/2/2015 09:30 AM in Courtroom 7B, 101 West Lombard Street, Baltimore, Maryland 21201, before Magistrate Judge Timothy J. Sullivan. Signed by Magistrate Judge Timothy J. Sullivan on 3/30/2015. (jks, Deputy Clerk)

15-0656 TJS

AO 91 (Rev 11/11) Criminal Complaint

SEALED BY COURT ORDER

UNITED STATES DISTRICT COURT for the Northern District of California

ORIGINAL FILED

MAR 25 2015

United States of America v. CARL MARK FORCE IV, et al

Case No.

RICHARD W. WIEKING CLERK, U.S. DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA

3-15-70370

Defendant(s)

MEJ

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 2012 through 2013 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Table with 2 columns: Code Section and Offense Description. Rows include 18 U.S.C. Section 641 (Theft of Government Property), 18 U.S.C. Section 1343 (Wire Fraud), 18 U.S.C. Section 1956(h) (Money Laundering), and 18 U.S.C. Section 208 (Conflict of Interest).

FILED LOGGED ENTERED RECEIVED

MAR 30 2015

AT BALTIMORE CLERK U.S. DISTRICT COURT DISTRICT OF MARYLAND

Handwritten signature of a deputy clerk.

This criminal complaint is based on these facts:

See Affidavit of Special Agent Tigran Gambaryan (attached)

Handwritten signature of Kathryn Haun.

Approved as to form:

AUSA Kathryn Haun

Continued on the attached sheet.

Handwritten signature of the complainant.

Complainant's signature

S/A Tigran Gambaryan, IRS-Criminal Investigations Printed name and title

Sworn to before me and signed in my presence.

Date: 03/25/2015

Handwritten signature of Judge Maria-Elena James.

Judge's signature

City and state: San Francisco, CA

Hon. Maria-Elena James, U.S. Magistrate Judge

Printed name and title

1 MELINDA HAAG (CABN 132612)  
United States Attorney

2 DAVID R. CALLAWAY (CABN 121782)  
3 Chief, Criminal Division

4 KATHRYN HAUN (DCBN 484131)  
WILLIAM FRENTZEN (LABN 24421)  
5 Assistant United States Attorneys

6 450 Golden Gate Avenue, Box 36055  
San Francisco, California 94102-3495  
7 Telephone: (415) 436-7200  
8 FAX: (415) 436-7234  
Kathryn.haun@usdoj.gov  
William.frentzen@usdoj.gov

9 RAYMOND N. HULSER (MABN 551350)  
10 Acting Chief, Public Integrity Section

11 RICHARD B. EVANS (DCBN 441494)  
12 Trial Attorney

13 1400 New York Avenue, N.W.  
Washington, D.C. 20005  
14 Telephone: (202) 353-7760  
Richard.B.Evans@usdoj.gov

15 Attorneys for United States of America

16 UNITED STATES DISTRICT COURT  
17 NORTHERN DISTRICT OF CALIFORNIA  
18 SAN FRANCISCO DIVISION

20 UNITED STATES OF AMERICA,

21 v.

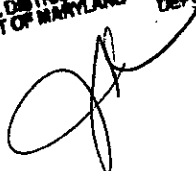
22 CARL M. FORCE IV and  
SHAUN W. BRIDGES,

23 Defendants.  
24

) AFFIDAVIT OF SPECIAL AGENT TIGRAN  
) GAMBARYAN IN SUPPORT OF CRIMINAL  
) COMPLAINT

) FILED UNDER SEAL

25  
26 I, Tigran Gambaryan, being first duly sworn, hereby depose and state as follows:  
27  
28

FILED ENTERED  
LOGGED RECEIVED  
MAR 30 2015  
AT BALTIMORE  
CLERK U.S. DISTRICT COURT  
DISTRICT OF MARYLAND  
BY  DEPUTY

1 **I. INTRODUCTION AND AGENT BACKGROUND**

2 The following affidavit is made in support of a criminal complaint and arrest warrant for Carl  
3 Mark FORCE IV ("FORCE") for violations of 18 U.S.C. Section 1343 (Wire Fraud); 18 U.S.C. Section  
4 641 (Theft of Government Property); 18 U.S.C. Section 1956 (Money Laundering); and 18 U.S.C.  
5 Section 208 (Conflict of Interest) and also in support of a criminal complaint and arrest warrant for  
6 Shaun W. BRIDGES ("BRIDGES") for violations of 18 U.S.C. Section 1343 (Wire Fraud) and 18  
7 U.S.C. Section 1956 (Money Laundering).

8 I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service  
9 (IRS), in the Northern District of California and have been since 2011. I am currently the group's Cyber  
10 Crimes Unit Liaison. Prior to that, my background was as an auditor for California's Franchise Tax  
11 Board where I investigated abusive tax shelters. My training and experience includes, but is not limited  
12 to, investigations involving money laundering, white collar fraud, public corruption, organized crime,  
13 and violations of the Bank Secrecy Act and tax code. I have developed a specialty in cyber and digital  
14 currency crimes.

15 I am involved in an investigation into members of the Baltimore Silk Road Task Force to include  
16 former Drug Enforcement Administration Agent Carl Mark FORCE IV (FORCE) and former Secret  
17 Service Agent Shaun BRIDGES (BRIDGES). This is a bicoastal investigation that is based in San  
18 Francisco, being handled by the U.S. Attorney's Office for the Northern District of California and the  
19 Public Integrity Section in Washington D.C.

20 In this investigation, I am joined by several co-case agents, to include Special Agents and a Staff  
21 Operations Specialist from the Federal Bureau of Investigation (FBI) San Francisco Division's Public  
22 Corruption Squad, which investigates abuse of public office in violation of criminal law to include  
23 fraud, bribery, extortion, conflicts of interest, and embezzlement. I am also joined in this investigation  
24 by the Department of Justice's Office of the Inspector General (DOJ OIG) and the Department of  
25 Homeland Security's Office of the Inspector General (DHS OIG), both of which investigate and  
26 prosecute fraud and abuse by federal officials.

27 The facts in this affidavit come from my personal observations, my training and experience, and  
28 information obtained from other agents and witnesses. This affidavit is intended to show merely that

1 there is sufficient probable cause for the requested complaint and warrants and does not set forth all of  
2 my knowledge about this matter.

## 3 II. SUMMARY

4 The government had multiple investigations into the Silk Road marketplace, an underground  
5 black market that allowed vendors and buyers to conduct illegal transactions over the internet. One of  
6 these investigations was conducted in the Southern District of New York, and the other was conducted  
7 out of Baltimore in the District of Maryland. Both FORCE and BRIDGES were assigned to the  
8 Baltimore investigation and not the New York investigation. The two investigations were conducted  
9 independently of each other.

10 Throughout 2012 and 2013, both FORCE and BRIDGES had significant responsibilities related  
11 to Baltimore's investigation. In this capacity, FORCE was the lead undercover agent in communication  
12 with DPR, the owner, administrator and operator of the Silk Road website.<sup>1</sup> BRIDGES was the  
13 computer forensics expert on the Baltimore investigation. In their capacity as members of the Baltimore  
14 Silk Road Task Force, both FORCE and BRIDGES had significant exposure to and developed expertise  
15 in the digital currency known as Bitcoin.

16 As will be described further herein, FORCE and BRIDGES abused their positions as federal  
17 agents and engaged in a scheme to defraud a variety of third-parties, the public, and the government, all  
18 for their own financial enrichment. With respect to former Drug Enforcement Administration (DEA)  
19 Special Agent FORCE, the investigation has revealed among other things that:

- 20 a. FORCE created certain fictitious personas -- that were not officially sanctioned -- to  
21 communicate with DPR, the target of FORCE's investigation. Using one of these  
22 personas, FORCE sought to extort DPR by seeking monetary payment, offering in  
23 exchange not to provide the government with certain information if DPR paid \$250,000;
- 24 b. FORCE acted outside the scope of his official role on the Baltimore Silk Road Task  
25 Force and created a fictitious persona named "French Maid." Operating as "French  
26

27 <sup>1</sup> Until October 1, 2013, DPR was known to FORCE and the rest of the Baltimore Silk Road  
28 Task Force only by his online moniker "Dread Pirate Roberts" or "DPR." Ulbricht was known on the  
Silk Road site by the moniker "Dread Pirate Roberts" (DPR) and is referred to hereafter interchangeably  
as "DPR" and "Ulbricht."

1 Maid,” FORCE fraudulently represented to DPR certain information concerning “French  
2 Maid’s” true identity and offered to sell DPR information about the government’s  
3 investigation into Silk Road in exchange for approximately \$100,000 worth of bitcoin,  
4 which DPR paid and FORCE deposited into his own personal accounts;

5 c. FORCE stole and converted to his own personal use a sizeable amount of bitcoins that  
6 DPR sent to FORCE in FORCE’s official undercover capacity and rather than turning  
7 those bitcoin over to the government, FORCE deposited them into his own personal  
8 accounts;

9 d. FORCE engaged in a series of complex transactions between various Bitcoin accounts  
10 (known as Bitcoin addresses), his personal digital currency accounts, and his personal  
11 bank accounts, including a \$235,000 wire to an overseas account in Panama, all in an  
12 effort to launder and conceal the true source of the ill-gotten proceeds;

13 e. FORCE used his official position as a DEA agent to illegally run criminal history checks  
14 on individuals for the benefit of a third-party digital currency exchange company,  
15 CoinMKT, in which FORCE had personally invested approximately \$110,000 worth of  
16 bitcoin;

17 f. FORCE functioned as the de facto Chief Compliance Officer for CoinMKT all the while  
18 employed as a DEA agent, even allowing himself to be featured in CoinMKT’s “pitch  
19 decks” to venture capital investors and allowing himself to be listed as CoinMKT’s anti-  
20 money laundering and/or compliance officer in order to benefit CoinMKT (a company in  
21 which FORCE had invested);

22 g. FORCE improperly directed CoinMKT to freeze one of its individual customer’s  
23 accounts containing a large amount of digital currency, worth approximately \$297,000,  
24 even though he lacked a sufficient legal basis on which to do so, and FORCE then  
25 illegally seized those funds and transferred them into his own personal account; and

26 h. FORCE used his supervisor’s signature stamp, without authorization, on an official U.S.  
27 Department of Justice subpoena and sent the subpoena to a payments company, Venmo,  
28 directing the company to unfreeze his own personal account, which had been previously

1 frozen due to certain suspicious activity. FORCE then sought to conceal evidence of his  
2 improper use of an official subpoena by directing the company not to contact the DEA  
3 and attempting to destroy copies of the subpoena. When the company did not comply,  
4 FORCE asked another agent on the Baltimore Silk Road Task Force, an IRS agent, to  
5 collaborate with him on seizing that company's bank accounts.

6 With respect to former U.S. Secret Service (USSS) Special Agent BRIDGES, the investigation  
7 has revealed among other things that:

- 8 a. In late January 2013, members of the Baltimore Silk Road Task Force, to include  
9 BRIDGES and FORCE, gained access to a Silk Road website administrator account as a  
10 result of the arrest of a former Silk Road employee. On January 25, 2013, the Silk Road  
11 website suffered a sizeable theft of bitcoins, bitcoins which were moved into Mt. Gox, a  
12 digital currency exchange based in Japan;
- 13 b. On February 12, 2013, BRIDGES formed and registered a personal limited liability  
14 company called "Quantum International Investments, LLC," (Quantum), and on February  
15 22, 2013, BRIDGES opened an account at Fidelity Investments (Fidelity) in the name of  
16 Quantum;
- 17 c. According to records obtained from Fidelity, BRIDGES funded his Quantum Fidelity  
18 account exclusively with wire deposits from Mt. Gox in Japan. Specifically, between  
19 March 6, 2013 through May 7, 2013, BRIDGES' Quantum Fidelity account in the United  
20 States received nine wire transfers from Mt. Gox totaling approximately \$820,000;
- 21 d. Despite having personally benefitted in the amount of \$820,000 from a Mt. Gox account  
22 and receiving a large wire on May 7, 2013 from Mt. Gox, just two days later on May 9,  
23 2013, BRIDGES served as the affiant on a multi-million dollar seizure warrant for Mt.  
24 Gox and its owner's bank accounts; and
- 25 e. Upon learning of the government's criminal investigation into the Baltimore Silk Road  
26 Task Force based in the Northern District of California, and following an interview by  
27 the FBI as part of the criminal investigation, BRIDGES transferred over \$250,000 out of  
28

1 his Quantum Fidelity account via wire transfers into another bank account held by  
2 himself and a third-party.

3 Because this affidavit is for the limited purpose of establishing probable cause for the crimes  
4 proposed to be charged at the present time, it does not include certain additional facts known to me and  
5 the government's investigation continues.

### 6 III. RELEVANT STATUTES

7 Based on my training and experience and the facts as set forth in this affidavit, there is probable  
8 cause to believe that FORCE has committed violations of law to include Title 18, United States Code,  
9 Section 1343 (Wire Fraud), Title 18, United States Code, Section 641 (Theft of Government Property),  
10 Title 18, United States Code, Section 1956 (Money Laundering), and Title 18, United States Code,  
11 Section 208 (Conflict of Interest). There is also probable cause to believe that BRIDGES has committed  
12 violations of law to include Title 18, United States Code, Section 1343 (Wire Fraud) and Title 18,  
13 United States Code, Section 1956 (Money Laundering).

14 **Title 18 U.S.C. § 641** prohibits embezzling, stealing, or converting any property belonging to the  
15 United States worth more than \$1,000. The essential elements of this offense are: (1) the defendant  
16 knowingly embezzled, stole, or converted to the defendant's use or the use of another the money or  
17 property of value with the intention of depriving the owner of the use or benefit of the money or  
18 property; (2) the money or property belonged to the United States; and (3) the value of the money or  
19 property was more than \$1,000. See Ninth Circuit Instruction 8.39.

20 **Title 18 U.S.C. § 1343** prohibits wire fraud. The essential elements of this offense are: (1) the  
21 defendant knowingly participated in, devised or intended to devise a scheme or plan to defraud, or a  
22 scheme or plan for obtaining money or property by means of false or fraudulent pretenses,  
23 representations, or promises; (2) the statements made or facts omitted as part of the scheme were  
24 material, that is they had a natural tendency to influence, or were capable of influencing, a person to part  
25 with money or property; (3) the defendant acted with the intent to defraud, that is, the intent to deceive  
26 or cheat; and (4) the defendant used, or caused to be used, a wire communication to carry out or attempt  
27 to carry out an essential part of the scheme. See Ninth Circuit Instruction 8.124.





1 long period beginning April 2013 through May 2014.<sup>2</sup> This does not include amounts deposited from  
2 May 2014 onward. I have also learned through my investigation that during this timeframe FORCE  
3 paid off his mortgage, a government thrift savings plan loan, and wrote several very large checks for  
4 tens of thousands of dollars. In 2014, FORCE made investments in real properties, in businesses, and  
5 wired hundreds of thousands of dollars into an overseas account.

6 From 2013 through the present, FORCE has held numerous accounts in his own name and with  
7 his own personal identifiers<sup>3</sup> at a variety of digital currency exchanges around the world, including in the  
8 Northern District of California. Moreover, in April 2014, FORCE established a company called Engedi,  
9 LLC. According to documents filed with the Maryland Secretary of State, Engedi, LLC's purpose is to  
10 speculate and invest in Bitcoin.

11 Like FORCE, BRIDGES was a member of the Baltimore Silk Road Task Force. Until his abrupt  
12 resignation on March 18, 2015, after learning he was a subject of this investigation, BRIDGES was  
13 employed as a U.S. Secret Service (USSS) Special Agent for approximately six years. He began his  
14 career with USSS in October 2009 and served in its Baltimore Field Office. After the Baltimore Silk  
15 Road Task Force ended, BRIDGES remained part of the USSS Electronic Crimes Task Force in  
16 Maryland. In this role, he served as the affiant on numerous seizure warrants.

17 On January 25, 2013, the Silk Road website suffered a sizeable theft of Bitcoin, a theft with  
18 which BRIDGES was associated. For reasons discussed below, I believe the proceeds of this theft were  
19 transferred to the Mt. Gox exchange in Japan. On February 12, 2013, not long after the Silk Road thefts  
20 occurred, BRIDGES formed a company called Quantum International Investments, LLC (Quantum).  
21 On February 22, 2013, BRIDGES established a personal investment account at Fidelity Investments  
22 (Fidelity) in the name of Quantum.

23 BRIDGES used that Fidelity account to receive several large international wire transfers from  
24 Japan, specifically from Mt. Gox, throughout the March through May 2013 timeframe. There were nine  
25

26  
27 <sup>2</sup> Approximately \$330,000 was deposited in 2013 and approximately \$427,000 was deposited in  
28 2014. This does not include the deposits made after this period that are discussed further below.

<sup>3</sup> These personal accounts use FORCE's home address, and link to his personal bank and email  
account information.

1 wire transfers from Mt. Gox to BRIDGES' Quantum Fidelity account, and each was just under  
2 \$100,000. This account was funded exclusively with deposits from Mt. Gox.

3 Just two days after receiving his last Mt. Gox wire on May 7, 2013, BRIDGES served in his  
4 official capacity as the affiant on a May 9, 2013 seizure warrant where he seized over \$2.1 million from  
5 Mt. Gox, under the theory Mt. Gox was operating in violation of 18 U.S.C. Section 1960, which  
6 prohibits the operation of an unregistered money service business.

7 After learning of this investigation into the Baltimore Silk Road Task Force and after being  
8 interviewed by federal law enforcement in the summer of 2014, BRIDGES transferred via two separate  
9 interstate wires over \$250,000 from his Quantum Fidelity account into an account at another bank that  
10 was held in his own name and in the name of a third-party (with whom BRIDGES has a personal  
11 relationship).

## 12 V. BITCOIN BACKGROUND

13 Bitcoin<sup>4</sup> is a form of decentralized, convertible virtual currency that exists through the use of an  
14 online, decentralized ledger system. While Bitcoin mainly exists as an internet-based form of currency,  
15 it is possible to "print out" the necessary information and exchange Bitcoin via physical medium. The  
16 currency is not issued by any government, bank, or company, but rather is generated and controlled  
17 through computer software operating via a decentralized network. To acquire bitcoins, a typical user  
18 will purchase them from a Bitcoin seller or "exchanger." It is also possible to "mine" bitcoin by  
19 verifying other users' transactions. Bitcoin is just one form of digital currency, and there are a  
20 significant number of other varieties of digital currency.

21 Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value  
22 from government regulation or law), or other convertible virtual currencies in order to obtain bitcoins.  
23 When a user wishes to purchase bitcoins from an exchanger, the user will typically send payment in the  
24 form of fiat or other convertible virtual currency to an exchanger, usually via wire or ACH, for the  
25 corresponding number of bitcoins based on a fluctuating exchange rate. The exchanger, often for a  
26

27 <sup>4</sup> Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to  
28 use "Bitcoin" (singular with an upper case letter B) to label the protocol, software, and community, and  
"bitcoin" or "bitcoins" (with a lower case b) to label units of the currency and that practice is adopted  
here:

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

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

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

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

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

## 22 VI. SILK ROAD BACKGROUND

23 The Silk Road website was established in early 2011 and operated until on or about October 2,  
24 2013, when it was seized by law enforcement. The illegal nature of the commerce hosted on Silk Road  
25 was readily apparent to anyone visiting the site. The vast majority of the goods for sale consisted of  
26 illegal drugs of nearly every variety, openly advertised on the site as such and prominently visible on the  
27 home page. The only form of payment accepted on Silk Road was Bitcoin.

1 Silk Road was only accessible through the TOR network, a special network on the internet  
2 designed to conceal the true IP addresses of the computers on the network, and, thereby, the identities of  
3 the network's users. TOR stands for "The Onion Router."

4 Every Silk Road user had at least one Bitcoin address associated with the user's Silk Road  
5 account, where deposits to the account could be sent. To make purchases on the site, the user first had  
6 to obtain Bitcoin (for example, from an exchanger) and have them sent to the bitcoin deposit address  
7 associated with the user's Silk Road account. After thus funding the account, the user could make  
8 purchases from Silk Road vendors.

9 A federal grand jury sitting in the Southern District of New York indicted Ross William  
10 Ulbricht, also known as "DPR," as being the creator of Silk Road and engaging in a drug conspiracy in  
11 violation of 21 U.S.C. Section 846, among other charges. The matter proceeded to a multi-week trial in  
12 January 2015 before U.S. District Judge Katherine B. Forrest. Evidence at that trial, and other evidence  
13 of which I am aware, establishes that from late 2012 through his arrest on October 1, 2013, Ulbricht  
14 (DPR) was residing in and ran the Silk Road from San Francisco. On or about February 4, 2015, a  
15 federal jury sitting in the Southern District of New York convicted Ulbricht of all counts with which he  
16 was charged. Sentencing is set for May 15, 2015. ADDITIONAL PARAGRAPH PROVIDED TO  
17 COURT IN SEPARATE UNDER SEAL FILING IS REDACTED HERE.

18 Aside from the New York case, on October 1, 2013, the District of Maryland charged Ulbricht  
19 with murder-for-hire and related drug-conspiracy charges.<sup>5</sup> It is the District of Maryland's investigation  
20 and case in which FORCE and BRIDGES were involved.

## 21 **VII. FORCE PROBABLE CAUSE**

### 22 **FORCE's Official Undercover Role On Baltimore's Silk Road Task Force**

23 As described above, FORCE, BRIDGES, and other law enforcement agents from the Department  
24 of Homeland Security, Internal Revenue Service, and the U.S. Postal Inspection Service,<sup>6</sup> worked on a

25 \_\_\_\_\_  
26 <sup>5</sup> The District of Maryland had previously charged "John Doe a/k/a Dread Pirate Roberts" with  
27 these charges on or about May 1, 2013, at which time the District of Maryland was unsure of the true  
identity of DPR. The District of Maryland subsequently charged Ulbricht with these offenses after an  
IRS Special Agent on the Southern District of New York's investigation identified DPR as Ulbricht.

28 <sup>6</sup> The Bureau of Alcohol, Tobacco & Firearms (ATF) was part of the Baltimore Silk Road Task  
Force early on, but their involvement did not last long.

1 task force out of Baltimore dedicated to identifying and apprehending DPR, later determined to be Ross  
2 Ulbricht.

3 As part of his official role in the Baltimore Silk Road investigation, FORCE communicated with  
4 DPR using an undercover identity, hereafter referred to as "Nob." Nob (FORCE) and DPR  
5 communicated throughout 2012 and 2013 using a variety of methods of communication, including on a  
6 private messaging system on the Silk Road website and on chat programs that operated over the TOR  
7 network. Their communications reveal that DPR believed Nob to be a drug smuggler operating in the  
8 United States with connections to criminal organizations throughout the world. In reality, of course,  
9 Nob was FORCE, an undercover DEA agent. Many but not all of their communications were encrypted,  
10 as discussed further below.

11 Some portion of the communications between DPR and Nob (FORCE) are memorialized in  
12 FORCE's official case file, preserved in what are known as DEA 6s, which are official reports of the  
13 DEA's investigation. Some of the communications are also preserved on FORCE's official computers.  
14 However, not all of the communications between DPR and Nob (FORCE) were memorialized.

15 At the time of Ulbricht's arrest, law enforcement seized a laptop computer from Ulbricht's  
16 person. This computer has been forensically analyzed. It, too, contained evidence of communications  
17 between DPR and Nob (FORCE). It also contained certain communications between DPR and FORCE  
18 that FORCE did not memorialize in his official reports or as part of his official case file.

19 Ulbricht's computer also contained a handful of files that appear to be Ulbricht's notes to  
20 himself. One such file is named "LE counterintel" which your affiant believes stands for "Law  
21 Enforcement Counterintelligence" and contains information that DPR was receiving from purported  
22 "inside" law enforcement sources. I have reviewed these files and believe that they contain information  
23 that came from a person or persons inside law enforcement, in part because of their substance and in part  
24 because of their use of certain terminology and acronyms that are not widely known by the public.

1 Prior to his arrest, DPR was known to have been hiding his true identity and location from law  
2 enforcement, so information concerning the government's investigation was material and valuable to  
3 him.

4 I have reviewed many of the communications between DPR and Nob (FORCE) that are  
5 available. At some point, Nob (FORCE) and DPR began encrypting certain of these communications  
6 using what is known as PGP encryption. PGP stands for "pretty good privacy" and is an encryption  
7 algorithm that allows its users to send encrypted conversations through messaging or chat services.  
8 Much like the way bitcoins are controlled, PGP too uses a system of public keys and private keys. With  
9 PGP, a public key is used to encrypt a message for a specific user to read, and a private key is used by  
10 the recipient to decrypt the message. In addition to needing a private key to decrypt a message, a user  
11 must also possess a unique password that was established at the time of creation to decrypt or sign a  
12 message.

13 A review of FORCE's official case file does not contain any of the private PGP keys or  
14 passwords needed to decrypt FORCE's encrypted communications with DPR. Nor did FORCE provide  
15 these private PGP keys to the prosecutor on the Baltimore case or to those in his chain-of-command.  
16 Instead, FORCE appears to have been the only individual to have possessed the private PGP keys and  
17 passwords needed to unlock his communication with DPR. This is notable, because as a law  
18 enforcement agent, I know that one of the chief concerns in working an investigation and building  
19 evidence is the ability to obtain decipherable, admissible evidence for use in later proceedings.

20 Despite his involvement in the Baltimore Silk Road investigation, and knowledge that other law  
21 enforcement would be unable to read encrypted communications without the private PGP keys, FORCE,  
22 acting as Nob, specifically instructed DPR to use PGP to encrypt messages relating to the investigation.  
23 While this request may have enhanced Nob's (FORCE's) credibility to DPR as a "criminal," thereby  
24 furthering his cover, it would have made it difficult for FORCE to document the communications,  
25 communications that would be of use to law enforcement making a case against DPR at a later date.  
26 Even if encrypting messages to DPR would make Nob more credible, the communications should have  
27 been documented, in deciphered form, and memorialized in the case file.

1 I have conferred with other law enforcement agents who conduct online undercover operations  
2 and believe the failure to preserve the private PGP keys while simultaneously directing a target to use  
3 PGP to encrypt messages makes little sense in the context of a law enforcement investigation,  
4 particularly taking into account that this task force involved multiple law enforcement officers, all of  
5 whom might require access to the evidence FORCE gathered in his dealings with DPR: In the event  
6 FORCE were to lose the PGP private keys, or that something were to happen to FORCE, any evidence  
7 contained in the encrypted PGP format would effectively be lost and unusable without the private key.  
8 FORCE's apparent failure to document the private PGP keys for his communications with DPR  
9 anywhere in his case file, or to provide them to others at the DEA or to the prosecutor, leads me to  
10 believe he did not want anyone other than himself (FORCE) to be able to decrypt certain of those  
11 communications, and that, as a result, he sought deliberately to undermine the integrity of the ongoing  
12 Baltimore Silk Road Task Force investigation.

13 Although in the beginning of his time communicating with DPR, FORCE (as Nob) occasionally  
14 provided certain decrypted communications to others on the Task Force, including the prosecutor with  
15 whom he was working, FORCE did not provide all communications in decrypted form. This was  
16 despite the fact that the prosecutor with whom FORCE was working repeatedly emphasized the need for  
17 FORCE to provide all encrypted communications. In fact, toward the end of the timeframe in which  
18 Nob (FORCE) was in relatively heavy communication with DPR, FORCE increasingly was not  
19 providing the decrypted versions of their communication.

20 **FORCE's Theft of 525 Bitcoins Coming from Ulbricht, a/k/a "DPR"**

21 In his communications with DPR, Nob (FORCE) created the fiction that Nob had sensitive  
22 information that he would provide to DPR, often in exchange for payment, including law enforcement  
23 sensitive information.

24 One of the cover stories that Nob (FORCE) created with DPR was that Nob had access to a  
25 corrupt government employee, fictionally named "Kevin." Ironically, "Kevin" was supposed to be a  
26 corrupt Department of Justice case agent on the government's Silk Road investigation and  
27 simultaneously on Nob's payroll, who would feed Nob information about law enforcement's  
28



1 investigation into the Silk Road. FORCE memorialized this cover story concerning "Kevin" in a DEA 6  
2 dated August 1, 2013 (the "August DEA 6").

3 DPR subsequently paid Nob (FORCE) in bitcoins on at least two occasions. One payment was  
4 in June 2013 for 400 bitcoins<sup>7</sup> for fraudulent identification documents that Nob was supposed to provide  
5 to DPR. A second payment was in August 2013 for 525 bitcoins for "Kevin's" inside law enforcement  
6 information. At the time of the payments, 400 bitcoins would have been worth approximately \$40,000  
7 and 525 bitcoins would have been worth approximately \$50,000.<sup>8</sup> Both the June 400 bitcoin payment  
8 and the August 525 bitcoin payment became official government property once DPR made the  
9 payments: they were received as part of FORCE's official undercover role from the target of a federal  
10 investigation and therefore became undercover proceeds.

11 As is described further below, rather than properly documenting these payments, and  
12 safeguarding them in a government account, FORCE took custody of the payments and deposited the  
13 bulk of the 400 bitcoin payment and all of the 525 bitcoin payment into his own personal account.  
14 Records received from a digital currency exchange, CampBX, reveal that FORCE maintained a personal  
15 account there that was linked directly to two additional personal accounts belonging to FORCE: (1)  
16 FORCE's account at another digital currency exchange, Bitstamp, and (2) FORCE's account at a  
17 payments processing account, Dwolla, neither of which were government or official accounts.<sup>9</sup>

18 In the August DEA 6, FORCE memorialized the fact that he, acting as Nob, sent a PGP-  
19 encrypted communication to DPR. According to the August DEA 6, Nob (FORCE) "advised DPR that  
20

---

21 <sup>7</sup> The 400 bitcoin payment was actually an 800 bitcoin payment but Nob (FORCE) refunded  
DPR 400 bitcoins because the deal for the fraudulent identification documents allegedly fell through.

22 <sup>8</sup> These are very conservative estimates and the actual loss amount is likely greater than these  
23 amounts: FORCE himself valued the 400 bitcoin payment as being equal to \$76,800 on October 22,  
24 2013, and not \$40,000 as described here. The reason for the difference concerns the fluctuating value of  
25 bitcoin during this timeframe. The value of bitcoin at the time of the June 2013 payment was  
26 approximately \$100 per bitcoin, yielding the \$40,000 approximation provided here. However, the value  
at the time of FORCE's own valuation of the 400 bitcoin payment in October 2013 was approximately  
\$192 per bitcoin. It should also be noted that during the time that FORCE was liquidating bitcoins  
through his own personal accounts, the value of bitcoin fluctuated dramatically ranging from less than  
\$300 per bitcoin to over \$1100 per bitcoin.

27 <sup>9</sup> FORCE maintained a separate account at Dwolla in the name of his official undercover  
28 identity. In contrast, FORCE's personal account at Dwolla was in his own name and established using  
his own personal identifiers such as Social Security number, home address, personal email and date of  
birth.

1 'Kevin' wanted a 'donation' of bitcoins from DPR, the inference being that the information on the Silk  
2 Road investigation is valuable." The August DEA 6 further specifies that "Special Agent FORCE  
3 provided a Bitcoin wallet address" for DPR to deposit the Bitcoin payment for "Kevin's" information.  
4 However, FORCE made an "Agent's Note" at the bottom of the August DEA 6 explicitly stating that  
5 DPR never made the payment, writing "**AGENT'S NOTE: DPR made no such payment.**" (emphasis  
6 added).

7 The August DEA 6 is also notable for what information it does not contain. It does not include  
8 the actual Bitcoin public address that Nob (FORCE) provided to DPR to receive payment for "Kevin's"  
9 information. Including this information would have allowed other law enforcement agents to trace any  
10 payment if made. Nor does the August DEA 6 list or document the PGP encryption password that  
11 would be subsequently needed to decipher the encrypted communication between DPR and Nob  
12 (FORCE) concerning "Kevin's" information or the information surrounding the payment for that  
13 information.

14 However, certain communications between Nob (FORCE) and DPR were maintained on the  
15 server that hosted the Silk Road website, which the FBI imaged as part of the Southern District of New  
16 York investigation. I have obtained and reviewed a copy of that server and it contains the  
17 communications between Nob (FORCE) and DPR, including certain communications that FORCE does  
18 not appear to have memorialized in the official case file. The server contains a chain of messages  
19 between DPR and Nob (FORCE) from July 31, 2013 through August 4, 2013. With the exception of  
20 one message DPR authored, the messages in the chain are completely encrypted.

21 That sole unencrypted message in this chain is from DPR to Nob (FORCE). It is dated August 4,  
22 2013, and concerns a payment DPR made for "Kevin's" information. Specifically, DPR wrote: "I could  
23 not decrypt your second message, got an error. I could decrypt the first, **and have sent the 525 btc as**  
24 **requested.** Please keep me posted and you have my word that no one else knows anything about this.  
25 I'm sorry I didn't know how much to send before. I was afraid of offending if I sent too little and  
26 looking foolish if I sent too much. I hope I didn't make things too difficult for you." (emphasis added).

27 Within approximately two hours of DPR sending the message described above, Nob (FORCE)  
28

1 responded to DPR with an encrypted message but containing the unencrypted subject line, "use PGP!"  
2 As noted, PGP stands for "Pretty Good Privacy," an encryption mechanism. In other words, FORCE  
3 was directing DPR to encrypt his messages. Following the message containing the unencrypted subject  
4 line were a series of additional back and forth encrypted PGP messages between Nob (FORCE) and  
5 DPR.

6 I know from other law enforcement agents who conduct undercover operations on TOR and  
7 black market sites that there is little reason to direct a target who is using clear communication to instead  
8 use encrypted communication, and no reason to fail to document a decryption mechanism in the case file  
9 or share it with other agents, management, or the prosecutor.

10 Again, FORCE did not memorialize the PGP private encryption key that could be used to  
11 decipher the July 31-August 4, 2013, encrypted communication chain between himself and DPR  
12 anywhere in his case file or provide it to anyone else at the DEA or to the prosecutor with whom he was  
13 working. Furthermore, the last mention of DPR's payment for "Kevin's" information in FORCE's  
14 official DEA case file is the August DEA 6, in which FORCE specifically stated that no payment was  
15 ever received. Nor are there any subsequent DEA 6s correcting or amending this. In fact, a review of  
16 FORCE's official case file reveals that FORCE never documented having received a 525 Bitcoin  
17 payment from DPR, as DPR's August 4, 2013, communication to Nob (FORCE) states had occurred.

18 I believe that FORCE, acting as Nob, instructed DPR to use PGP encryption in part to conceal  
19 the fact that DPR actually had made a 525 bitcoin payment to Nob (FORCE) that FORCE was not  
20 detailing in his official law enforcement reports. This conclusion is bolstered by the fact that in the  
21 August DEA 6 FORCE took care to explicitly note the fact in the "AGENT'S NOTE: DPR made no  
22 such payment," and there is no subsequent DEA 6 in which FORCE states that DPR did transmit a 525  
23 bitcoin payment. It is further bolstered by the fact that FORCE does not appear to have memorialized  
24 the PGP encryption keys for his communications with DPR anywhere in the official case file. Finally,  
25 when DPR mentioned the 525 bitcoin payment in the August 4 communication, the first response  
26 FORCE acting as Nob gave was "use PGP!"

27 Notably, by late July 2013, the Baltimore Silk Road Task Force had been made aware that the  
28 FBI was seeking to obtain an image of the Silk Road server, and therefore FORCE may have had reason

1 to fear that any communications between himself and DPR would be accessible to the FBI in the event  
2 the FBI was successful in imaging the server.

3 Records obtained from FORCE's personal digital currency account at a digital currency  
4 exchange company, CampBX, reveal that on September 27, 2013, FORCE deposited the precise amount  
5 of 525 bitcoins into his own personal account at CampBX.<sup>10</sup>

6 I have performed an analysis of the block chain as it concerns the 525 bitcoin deposit to  
7 FORCE's personal CampBX account. The analysis reveals that the 525 bitcoins FORCE received into  
8 his own personal CampBX account was directly linked, through a series of transactions, to the 525  
9 bitcoin payment that DPR made on August 4, 2013, i.e. the same day DPR communicated to Nob  
10 (FORCE) that he had "sent the 525 BTC as requested."

11 Records from the Silk Road servers establish that this 525 bitcoin payment originated from  
12 DPR's Silk Road account on August 4, 2013. Specifically, the 525 bitcoin payment was split into four  
13 smaller payments and made in the following manner:

- 14 a. On August 4, 2013 at 22:05 UTC a payment of 203 bitcoins
- 15 b. On August 4, 2013 at 22:05 UTC a payment of 134 bitcoins
- 16 c. On August 4, 2013 at 22:05 UTC a payment of 61 bitcoins
- 17 d. On August 4, 2013 at 22:01 UTC a payment of 127 bitcoins

18 The 525 bitcoin payment went from four addresses and ultimately landed in a single pass-  
19 through account on September 1, 2013. The 525 bitcoin remained in the pass-through account from  
20 September 1, 2013 until September 27, 2013, when they were transferred into FORCE's personal  
21 account at CampBX. These transactions are depicted on "Trace of 525 Bitcoin Payment," attached as  
22 Exhibit B.

23 Notably, FORCE treated DPR's June 400 bitcoin payment differently from the way he treated  
24 the August 525 bitcoin payment. To be sure, FORCE wrongfully deposited substantial portions of both  
25

26 <sup>10</sup> The September 27, 2013 date has significance because email records I have reviewed indicate  
27 that, at the latest on September 27, 2013, FORCE learned that DPR was about to be apprehended as part  
28 of the separate New York investigation into the Silk Road. In response to learning this information,  
FORCE wrote to the prosecutor with whom he was working inquiring as to the true name and  
identifying information of DPR. To my knowledge, FORCE was not provided with that information on  
September 27, 2013 in response to his inquiry.

1 payments into his own personal account at CampBX, and later transferred them to another of his  
2 personal accounts at Bitstamp, another digital currency exchange where FORCE maintained a personal  
3 account. However, FORCE memorialized the 400 bitcoin payment in a DEA 6 (albeit many months  
4 after the June 400 bitcoin payment was made) and in January 2014 attempted to put together a seizure  
5 warrant for that 400 bitcoin payment. He did not do any of this for the 525 bitcoin payment.

6 And as part of the process of putting together a seizure warrant for the 400 bitcoin payment, the  
7 federal prosecutor with whom FORCE was working emailed FORCE on January 16, 2014, and asked  
8 him a series of questions, including where the 400 bitcoins physically were. FORCE replied in an email  
9 later that day that the 400 bitcoins were "at the DEA." Based on my review of records and an analysis  
10 of the block chain, this was not true. And, with respect to the 525 bitcoins, FORCE never made any  
11 attempt to memorialize the payment or to prepare a seizure warrant. The federal prosecutor with whom  
12 FORCE was working was unaware of any 525 bitcoin payment ever having been made, as were  
13 FORCE's superiors at the DEA.

14 As part of this investigation, a federal search warrant was issued to search various personal email  
15 facilities belonging to FORCE. One such email account contained what appears to be a note to himself  
16 saved in a drafts folder. This note references two transfers of bitcoin payments from DPR, one made in  
17 "June/July 2013 for the fraudulent UK identification" and one made on August 4, 2013, the same date  
18 that DPR transferred 525 bitcoins to Nob (FORCE). See Exhibit C attached ("Draft Note"). In other  
19 words, FORCE's own saved email note indicates there was a payment from DPR on August 4, 2013.<sup>11</sup>  
20 The note also appears to attempt to justify FORCE's conduct, noting that the government actually made  
21 money during the time FORCE retained the payments (presumably given the fluctuating value of  
22 Bitcoin).

23 At the time of the 525 bitcoin payment and during the time of the communications between Nob  
24 (FORCE) and DPR, I have confirmed via internet service provider records and a variety of other means  
25 that DPR (Ross Ulbricht) was physically located in San Francisco, in the Northern District of California.  
26

27 \_\_\_\_\_  
28 <sup>11</sup> For reasons that are currently unknown to me, FORCE characterized the August 4, 2013  
payment as being for 200 bitcoins. However, as demonstrated above, the August 4, 2013 payment was  
for 525 bitcoins.

1 Based on the fact that DPR paid 525 bitcoins to Nob (FORCE) in FORCE's official government  
2 capacity as an undercover agent on Baltimore's Silk Road case, and based on the fact that the 525  
3 bitcoins ultimately ended up in FORCE's personal account with CampBX, **there is probable cause to**  
4 **believe that FORCE embezzled, converted, or stole government property in violation of 18 U.S.C.**  
5 **Section 641.** Given that these bitcoins went through several different accounts, often for short periods  
6 of time, as depicted in Exhibit B, and sat idle in a pass-through account from September 1, 2013 through  
7 September 27, 2013, before making their way to FORCE's personal account with CampBX on  
8 September 27, 2013, **there is also probable cause to believe that FORCE was attempting to conceal**  
9 **the source of the true source of the proceeds, in violation of 18 U.S.C. Section 1956.**

#### 10 FORCE's Fraud as "French Maid"

11 The only officially-sanctioned undercover identity for FORCE to communicate with DPR was as  
12 Nob. Nob was the persona that was discussed in FORCE's official reports. "Nob" was also the persona  
13 of which others in FORCE's chain-of-command and the federal prosecutor on the Baltimore Silk Road  
14 case were aware.

15 When DPR was arrested in San Francisco, he was caught literally in the act of running the Silk  
16 Road on a laptop computer. The FBI seized and forensically examined that laptop and its contents were  
17 part of the government's proof at trial against Ulbricht. As discussed above, Ulbricht's laptop contained  
18 a text document entitled "LE counterintel," a record of sorts that he maintained about information he  
19 was receiving from apparent law enforcement "insiders" purporting to have knowledge about the  
20 government's investigation into the Silk Road. The file appears to contain cut and pasted sections of  
21 what the insiders were relaying to him through online chats or private messages.

22 One such insider used the moniker "French Maid." Notes in a file from Ulbricht's computer  
23 indicate that he paid "French Maid" approximately \$100,000 worth of bitcoin in exchange for a name  
24 that he was told Mark Karpeles had provided to law enforcement. Mark Karpeles was at the time the  
25 CEO of the now-defunct Mt. Gox digital currency exchange. The Baltimore Silk Road Task Force was  
26 attempting to arrange an interview of Karpeles during the July to August 2013 timeframe, in order to  
27 obtain any information Karpeles might have had concerning the operator of Silk Road.

1 Specifically, in a text document recovered from Ulbricht's computer titled "log," there is an  
2 entry dated September 13, 2013, in which Ulbricht wrote: "French Maid claims that mark karpeles has  
3 given my name to DHLS [sic]. I offered him \$100K for the name." Days later,<sup>12</sup> Ulbricht wrote "I paid  
4 French Maid \$100K for the name given to DHLS by karpeles." Our investigation has revealed that there  
5 is probable cause to believe that FORCE was "French Maid," a source that Ulbricht paid for inside  
6 information.

7 I have reviewed private messages between "French Maid" (FORCE) and DPR obtained from the  
8 Silk Road server imaged by the FBI. The messages span from August 26, 2013 through September 14,  
9 2013. The bulk of the messages are encrypted with PGP keys, but some early messages are not  
10 encrypted. In the first message in this thread, dated August 26, 2013, "French Maid" wrote to DPR: "I  
11 have received important information that you need to know asap. Please provide me with your public  
12 key for PGP. Carl." (Emphasis added).

13 Just four hours later, "French Maid" sent a follow-up message to DPR with the subject line  
14 "**Whoops!**" and a message stating "I am sorry about that. My name is Carla Sophia and I have many  
15 boyfriends and girlfriends on the market place. DPR will want to hear what I have to say ;) xoxoxo."  
16 (Emphasis added).

17 What follow are a series of back and forth encrypted messages between DPR and "French  
18 Maid." Of particular note, there are several encrypted messages between DPR and "French Maid" on  
19 September 13, 2013, with "French Maid" including the subject line "Hope you like." It is unclear  
20 whether "French Maid" ever provided DPR with any name. In the "log" file recovered from Ulbricht's  
21 computer, after the entry stating that he had "paid French maid \$100k for the name given to DHLS by  
22 karpeles," there is an entry stating: "He hasn't replied for 4 days." There is no further entry in the "log"  
23 file regarding "French Maid."

24 The fact that the Baltimore Silk Road Task Force was attempting to arrange an interview with  
25 Karpeles was not widely known in law enforcement circles. In other words, "French Maid" could not  
26 have been just anyone out of the universe of law enforcement. It had to have been someone who knew  
27

28 <sup>12</sup> The entry gives only the date range of "September 11-September 18" and does not provide an exact date.

1 about Baltimore's attempt to arrange an interview with Karpeles.<sup>13</sup> Based on emails I have reviewed,  
2 FORCE was one of a small group of individuals that knew of those discussions.

3 Additional pieces of circumstantial evidence prove that FORCE is "French Maid." Both "French  
4 Maid" and FORCE (operating as "Nob") used the exact same brand of PGP software, a free brand called  
5 GnuPG. There are different brands of PGP software so it is noteworthy that both FORCE (operating as  
6 "Nob") and "French Maid" used the same brand. Not only did FORCE and "French Maid" both use the  
7 same brand of PGP software, they also both used the same outdated version of that software, 1.4.12.  
8 Version 1.4.12 was released on January 2012, and was replaced with a new version by December 2012;  
9 and was one of several versions of GnuPG software.<sup>14</sup> As such, both "French Maid" and FORCE (as  
10 Nob) were using a specific, older version of the GnuPG software, and neither of them replaced it with  
11 the other (free) versions of GnuPG that came out thereafter.

12 I know based on conversations with another federal agent who is involved in undercover  
13 investigations that among TOR users and consumers of PGP software, v1.4.12 version was somewhat  
14 outdated by late August 2013 when "French Maid" appeared in communication with DPR for the first  
15 time. This is not akin, for example, to two people using the same model of mobile phone but both  
16 having software that is out of date. Rather, the outdated version that both "French Maid" and FORCE  
17 (as Nob) used is more of a "signature" given the greater number of versions available.

18 There are also additional similarities between FORCE's (Nob's) and "French Maid's" PGP  
19 patterns. Both "Nob" and "French Maid" left certain default settings on their PGP software. For one  
20 thing, both "French Maid" and FORCE (Nob) left a "tag" that appeared on every message authored from  
21 their PGP key revealing the brand and version of PGP software they were using. This is akin to, for  
22 example, leaving the phrase "sent from my iPhone" on the bottom of one's emails but with greater  
23 detail: it would be akin to leaving a phrase like "sent from my iPhone 6 IOS 8.0.1." Leaving this "tag"  
24 on typically reveals that one is dealing with a fairly inexperienced user of PGP, because someone that  
25 regularly uses PGP to communicate would normally have changed their settings to omit this tag. After  
26

27 <sup>13</sup> My understanding is that that the interview with Karpeles never materialized.

28 <sup>14</sup> FORCE's investigation into Silk Road began in approximately February 2012 and he began  
using PGP as "Nob" sometime by approximately April 2012.



1 all, the entire point behind PGP software is anonymity, so if a user leaves the brand, version, bit, and  
2 release date of software on a message this is revealing something about the sender and undermines the  
3 goal of remaining 100% anonymous. One of the first things many PGP forums or regular users of PGP  
4 software instruct is that a user disable this feature. Moreover, PGP offers choices of 1024, 2048, 3072  
5 or 4096 bit encryption keys, with the higher keys giving greater protection. Many of the regular PGP  
6 users that were active on the Silk Road chose the 4096 bit keys because of the additional protection the  
7 larger key provided. Here both FORCE (as Nob) and "French Maid" used the 2048 bit default  
8 encryption key.

9 In addition to the PGP similarities, additional evidence that FORCE is "French Maid" is that the  
10 770 bitcoin payment DPR made to "French Maid," worth approximately \$98,000 at the time, ended up  
11 in FORCE's own personal digital currency account at CampBX. Specifically, Silk Road server data  
12 reveals that DPR made a payment on September 15, 2013, for 770 bitcoins. As noted, this is the same  
13 time frame when Ulbricht wrote in his journal that he had "paid French Maid \$100K for the name that  
14 [K]arpeles provided to DHLS."

15 An analysis of the block chain reveals that the 770 bitcoin payment was broken up into four  
16 separate bitcoin addresses and funneled through a series of pass-through accounts in September 2013.  
17 Between September 23, 2013 and September 29, 2013, those four addresses all came together to deposit  
18 770 bitcoins in FORCE's personal account at CampBX. For a detailed analysis of these complex  
19 transactions, see attached Exhibit E ("Trace and Analysis of DPR September 2013 Payment to French  
20 Maid"). Records obtained from CampBX demonstrate that this was an account held in FORCE's  
21 personal capacity.

22 Moreover, throughout November 2013, a substantial portion (at least 600 bitcoins) of the  
23 bitcoins in FORCE's CampBX account moved to FORCE's personal account at Bitstamp, a global  
24 digital currency exchange. Again here, records obtained from Bitstamp demonstrate that FORCE used  
25 his personal identifiers, home address, date of birth, personal bank account, and personal email address  
26 in connection with his Bitstamp account. As is discussed further below, FORCE subsequently  
27 liquidated hundreds of thousands of dollars worth of bitcoin from this Bitstamp account by having the  
28 proceeds wired into his personal checking account.

1 From having reviewed the entries from the "log" file on Ulbricht's computer and the  
2 unencrypted portion of the "French Maid" and DPR messages, I believe that FORCE's statement to  
3 DPR that he was "Carla Sophia," a user on the "market place" with "many girlfriends and boyfriends,"  
4 and FORCE's omission of his true identity, was a material misrepresentation. I believe this information  
5 influenced or was capable of influencing DPR whether to part with property, in this case 770 bitcoins,  
6 had DPR known that he was not communicating with a female named "Carla Sophia" but instead a male  
7 named Carl FORCE who was in fact a federal agent.

8 When DPR made the 770 bitcoin payment and when the communications between "French  
9 Maid" (FORCE) and DPR occurred, I have confirmed via internet service provider records and a variety  
10 of other means that DPR (Ulbricht) was physically located in San Francisco, in the Northern District of  
11 California. Based on the fact FORCE fraudulently told DPR via the use of interstate wires that he was  
12 "Carla Sophia," and that this fact was material, and given that on that basis DPR paid 770 bitcoins to  
13 "French Maid" for information, and that FORCE's personal accounts received 770 bitcoins from DPR  
14 during the same September 2013 timeframe, **there is probable cause to believe that FORCE**  
15 **committed wire fraud in violation of 18 U.S.C. Section 1343.** Given that, for example 194 bitcoins of  
16 this 770 payment went through several different accounts, as depicted in Exhibit E, from September 15,  
17 2013 through September 22, 2013, before making its way to FORCE's personal account with CampBX  
18 on September 23, 2013, **there is also probable cause to believe that FORCE was attempting to**  
19 **conceal the true source of the proceeds, in violation of 18 U.S.C. Section 1956.**

20 **FORCE's Extortion of DPR As "Death From Above"**

21 From reviewing one of FORCE's official reports dated November 12, 2012, I know that around  
22 that time FORCE obtained information from Homeland Security Investigations (HSI) about an  
23 individual then being considered as a possible suspect for DPR. The individual was named "AA."  
24 [actual name omitted here for confidentiality.] Due to its law-enforcement sensitive nature, FORCE was  
25 not permitted to share this information with individuals outside the government.

26 On or about April 1, 2013, FORCE created a fictitious persona on the Silk Road website named  
27 "Death from Above." FORCE, using the "Death from Above," moniker, solicited a \$250,000 payment  
28 from DPR and provided DPR the AA name and personal identifying details. Specifically, on April 1,

1 2013, "Death from Above" wrote DPR a message on the Silk Road server stating, "I know that you had  
2 something to do with [C.G.'s] disappearance and death. Just wanted to let you know that I'm coming  
3 for you. Tuque. You are a dead man. Don't think you can elude me. De Oppresso Liber."<sup>15</sup>

4 On April 6, 2013, DPR replied: "I don't know who you are or what your problem is but let me  
5 tell you one thing: I've been busting my ass every god damn day for over two years to make this place  
6 what it is. I keep my head down, I don't get involved with the drama . . . somehow psychotic people  
7 still turn up at my doorstep . . . I've been hacked, I've had threats made against the site and now, thanks  
8 to you, I've had threats made against my life. I know I am doing a good thing running this site. Your  
9 threats and all of the other psychos aren't going to deter me . . . stop messaging me and go find  
10 something else to do."

11 Later that day "Death From Above" (FORCE) replied to DPR, this time dropping a reference to  
12 AA's name, stating "It's not that easy [AA]. I'm legit. Green Beret. Friend of [C.G.]. I have access to  
13 TS/SCI files that FBI, DEA, AFP, SOCA would kill for. In fact, that is what I do . . . kill. The only  
14 thing that I do . . . Don't worry DoD has no interest in you and your little website. North Korea and Iran  
15 are a lot more important. In fact, as far as the Army and Navy are concerned you are a nobody. Petty  
16 drug dealer. But, [C.G.] was somebody. So tell me where he is and we will be done with this."

17 On April 10, 2013, "Death from Above" (FORCE) wrote to DPR again, this time giving DPR  
18 details concerning AA including full name, date of birth, citizenship, address, and other personal  
19 identifying details. DPR stated, "Is that enough to get your attention? After watching you, there is no  
20 way you could have killed [C.G.]. But I think you had something to do with it. So, \$250,000 in U.S.  
21 cash/bank transfer and I won't give your identity to law enforcement. Consider it punitive damages.  
22 Death From Above."

23 This payment appears to have never materialized, apparently because DPR did not believe  
24 "Death From Above's" information: in April 2013 Ulbricht wrote in the "log" file found on his laptop  
25  
26

27  
28 <sup>15</sup> The entire series of messages that "Death From Above" sent to DPR is not included here for  
brevity. The reference to C.G. [N.B. actual name omitted here for confidentiality] was a reference to an  
employee of DPR whom DPR had sought to have murdered in January 2013, as explained further below.

1 that he was "being blackmailed again. Someone says they have my ID, but hasn't proven it." Then, on  
2 April 11, 2013, Ulbricht wrote "guy blackmailing me who says he has my ID is bogus."

3 There appears to be no mention of "Death From Above" anywhere in FORCE's official DEA 6  
4 reports. However, FORCE's case file contains several DVDs of video taken with FORCE's official  
5 DEA laptop with a screen-recording program that shows certain communications with DPR. At some  
6 point in that several hours' worth of video footage there is a clip of a message being typed on the Silk  
7 Road using the "Death From Above" account. A screenshot from that video is attached as Exhibit A.  
8 Therefore, I believe FORCE was "Death From Above." Death From Above was not known to  
9 FORCE's superiors at the DEA, or the prosecutor assigned to the investigation, and FORCE was not  
10 authorized to disclose information concerning persons under investigation to anyone outside the  
11 investigative team, including, of course, disclosing information to the target himself as part of an  
12 unsanctioned extortion effort.

13 FORCE's acting as "Death From Above" demonstrates that FORCE had a history of: (1) creating  
14 fictitious personas that he did not memorialize in his official reports or apprise his superiors at the DEA  
15 or the prosecutor of; (2) soliciting payments from DPR; and (3) providing law-enforcement sensitive  
16 information to outside individuals when the disclosure of such information was not authorized and not  
17 memorialized in any official report.

#### 18 **FORCE's Conflict of Interest with CoinMKT**

19 CoinMKT is a California-based digital currency exchange company that supports trading  
20 between Bitcoin and other cryptocurrencies. I have reviewed a number of emails between FORCE and  
21 CoinMKT personnel, including its CEO and Co-Founder. These communications demonstrate that  
22 FORCE had a two-fold relationship with CoinMKT: he was both a major investor as well as its de facto  
23 compliance officer – all while he was employed as a full-time DEA agent who was investigating digital  
24 currency users and providers.

25 According to the emails, in November 2013 FORCE invested approximately \$110,000 worth of  
26 bitcoin in CoinMKT in two installments. First, on or about November 8, 2013, FORCE invested  
27 approximately \$10,000 worth of bitcoin in CoinMKT. Second, on or about November 25, 2013,  
28 FORCE invested approximately \$100,000 more worth of bitcoin in CoinMKT. According to CoinMKT,

1 the amount of FORCE's investment made him one of the top four investors in its first seed round of  
2 fundraising.

3 In addition to his investor status, FORCE was engaged in negotiations with CoinMKT to become  
4 its Chief Compliance Officer. Early on in their communications, CoinMKT's CEO flagged the  
5 possibility of a conflict with FORCE simultaneously being a DEA agent and serving as CoinMKT's  
6 compliance officer, noting in a November 1, 2013 email, "Just FYI if there's a work conflict - I'm not  
7 interested in doing anything illegal, so if we have to wait until you're not officially an employee [with  
8 DEA] or whatever, then let me know, you're the best judge of that...."

9 On November 16, 2013, CoinMKT's CEO wrote to FORCE asking a few questions. For  
10 example:

11 CoinMKT: Where would you work? Would you retain your old job?

12 FORCE: I would work here in Baltimore. I'm not sure how much longer I will be staying  
13 here at DEA.

14 CoinMKT: What connections can you bring to the table to help us with compliance?

15 FORCE: I have numerous contacts with IRS-Criminal Investigations, and my Intel Analyst  
16 (among others have direct access to FinCEN [Financial Crimes Enforcement  
17 Network]) . . . plus I can run queries in criminal databases [database name  
omitted] for suspect members of CoinMKT.

18 I know from my training and experience as a law enforcement officer that running checks in  
19 government databases such as the one FORCE referred to by name in the email above is strictly  
20 forbidden if not for an official law enforcement purpose. In fact, misuse of a government database may  
21 violate federal law and expose the offender to potential criminal liability. Nor does it appear that  
22 FORCE was speaking in the future tense about what he could do for CoinMKT down the road in the  
23 event he left the DEA and had full-time employment with CoinMKT, because his offer to run checks in  
24 criminal databases such as the one he mentioned by name would have been contingent upon his  
25 remaining an agent in order to have access to such databases.

26 Moreover, FORCE explicitly indicated that he would remain at DEA and simultaneously  
27 perform compliance work for CoinMKT. In a November 23, 2013, email FORCE stated "you know for  
28 right now, I think it would be better if you just pay me in stock options. I will stay on with DEA until

1 [CoinMKT] hits it 'big time' I have a lot of down time at DEA so I am confident that I can handle all  
2 that needs to be done regarding Legal and Compliance on a daily basis."

3 CoinMKT has advised that it needed a bank account in order to be successful in the digital  
4 currency field. On November 25, 2013, CoinMKT's CEO wrote to FORCE stating that a primary anti-  
5 money laundering (AML) contact was needed and asking if CoinMKT could list FORCE as its AML  
6 point of contact. Subsequently, on January 13, 2014, CoinMKT advised FORCE it was listing FORCE  
7 as its Compliance Officer for purposes of contact with a bank. FORCE responded the next day, "All  
8 right...let's hope this goes." Again, this was while FORCE was still employed as a DEA agent.

9 During the latter part of 2013, FORCE and CoinMKT continued to discuss FORCE's role as a  
10 Compliance Officer. By January 2014, email correspondence indicates that CoinMKT thought of and  
11 included FORCE as part of its core team, including him on internal emails. For example, in a January  
12 20, 2014, email CoinMKT's CEO sent to about 11 employees describing each employee's job  
13 description, FORCE was listed as the third person after the two founders as "compliance extraordinaire."  
14 Although CoinMKT authored this email, other communications demonstrate that FORCE thought of  
15 himself as one of the CoinMKT team and encouraged CoinMKT to use his status, his name, bio, and  
16 photo in their company materials. For example, on February 19, 2014, FORCE provided CoinMKT a  
17 headshot and bio to include in pitch decks for investors.<sup>16</sup> And on January 25, 2014, FORCE wrote  
18 inquiring if CoinMKT was registered with appropriate authorities and offering guidance about money  
19 transmission laws. In his email inquiry, FORCE used phrasing that suggested he was part of the  
20 company: "this will keep us from having the Feds seize any monies from us under 18 U.S.C. Section  
21 1960 . . . . eventually when we hit the big time, we are going to have to get a license from each state that  
22 we have customers in..." (emphasis added).

23 CoinMKT has provided numerous emails between CoinMKT and FORCE's personal email  
24 account. A search warrant was also obtained and served on Microsoft (which hosts Outlook email) for  
25 FORCE's personal emails. Some of the emails between FORCE and CoinMKT were included in the  
26 Microsoft production. However, several other of the emails that CoinMKT provided were not included

27  
28 <sup>16</sup> CoinMKT has confirmed that they used FORCE's bio and profile, and solicited venture fundraising in the San Francisco Bay Area, within the Northern District of California.

1 in the production that Microsoft made, including many of the emails excerpted above. The FBI has  
2 conferred with Microsoft about this issue, and was advised that all emails from FORCE's personal email  
3 were provided and that any emails that were missing likely meant that the user had deleted those emails.  
4 In other words, it appears to me that FORCE may have selectively deleted certain inculpatory emails  
5 between himself and CoinMKT.

6 **FORCE's Unlawful Seizure of R.P.'s Funds**

7 R.P. was a California resident who held an account at CoinMKT during at least 2013 and 2014.  
8 R.P. maintained cash in his account with CoinMKT as well as various brands of digital currency to  
9 include bitcoin, litecoin, feathercoin, and worldcoin.

10 On February 5, 2014, CoinMKT emailed FORCE regarding what it initially believed to be  
11 suspicious activity by R.P, noting that R.P. had withdrawn "\$10,000 three times instead of once for  
12 \$30,000." CoinMKT sought direction from FORCE on how to proceed, noting R.P. had approximately  
13 128 bitcoin (approximately \$109,000 at the time) in his account with CoinMKT.

14 On February 8, 2014, FORCE emailed CoinMKT directing them to suspend R.P.'s account and  
15 to "tell [R.P.] that the federal government is investigating him for federal violations of 18 USC 1956  
16 (money laundering) and 18 USC 1960 (unlicensed money transmitter) and 31 USC 5324  
17 (structuring).....I will seize the 128 btc federally and do all the paperwork...."

18 On or about February 7, 2014, FORCE instructed a DEA intelligence analyst to run a criminal  
19 history check on R.P., noting that the purpose was to uncover illegal activity on R.P. According to a  
20 subsequent report FORCE authored, the only information found on R.P. was that he had previously  
21 withdrawn \$17,000, had a felony conviction for vandalism, and was a self-employed actor.  
22 Nonetheless, on February 8, 2014, at FORCE's direction, CoinMKT froze R.P.'s account.

23 On February 10, 2014, FORCE, now using his official DOJ account instead of the personal email  
24 account he had historically used to communicate with CoinMKT, served an administrative subpoena on  
25 CoinMKT requesting that they provide all information regarding R.P. FORCE also sent the subpoena to  
26 CoinMKT by facsimile later that day. CoinMKT's facsimile services are hosted by "Hello Fax," a  
27 company based in San Francisco within the Northern District of California.

1 On February 11, 2014, CoinMKT's CEO emailed FORCE to relay that "some feedback from  
2 other users . . . may throw off our thesis about this user's [R.P.'s] activity. Let's talk when you can, I'm  
3 glad I caught this." CoinMKT's CEO has explained that he learned that a glitch in CoinMKT's system  
4 was not permitting users to withdraw more than \$10,000 worth of currency at a time, thereby  
5 diminishing the earlier suspicion that R.P. was structuring transactions or doing anything criminal.  
6 FORCE replied to this email, inquiring whether CoinMKT had frozen R.P.'s account and seeking  
7 information concerning R.P.'s digital currency balances, noting that R.P. may have a mental condition.

8 On March 1, 2014, R.P. wrote to CoinMKT advising that he had not been able to log in to his  
9 account. CoinMKT replied to R.P. that his account had been "suspended due to suspicious activity.  
10 Under government subpoena, we have been instructed to forward your communication to authorities.  
11 We have cc'd Mr. Carl FORCE who will be your point of contact, please send further communication to  
12 him to resolve this issue."

13 A Report of Investigation FORCE authored states that on February 26, 2014 and March 6, 2014,  
14 FORCE attempted to contact R.P. stating "I have attempted to contact you numerous times via telephone  
15 and emails, yet have received no response. I am trying to ascertain if your suspicious financial  
16 transactions at CoinMKT have a legitimate explanation. The facts show that you are structuring  
17 deposits and withdrawals. In addition, virtual currencies have been linked to illicit activities such as  
18 illegal narcotics transactions, money laundering, child pornography, etc. As such, I am starting the legal  
19 process to seize your Real Money Balances at CoinMKT. A negative response to this email will be  
20 evidence that you are abandoning your assets at CoinMKT."

21 Over the coming weeks, FORCE directed CoinMKT to seize R.P.'s account. CoinMKT has  
22 expressed it was hesitant to do so, but did not want to draw the ire of federal law enforcement, especially  
23 given that the digital currency field was already subject to fairly intense law enforcement scrutiny.  
24 CoinMKT also felt it prudent to defer to the direction of a federal law enforcement agent, and trusted  
25 that if FORCE was telling CoinMKT that R.P. was using their company as a platform for illegal  
26 activities, it was not in a position to second guess that conclusion. Nonetheless, CoinMKT requested  
27 something in writing from FORCE before seizing R.P.'s account.



1 During this March 2014 timeframe, R.P.'s account with CoinMKT contained two forms of  
2 currency. First, it contained approximately \$37,000 in cash. Second, it contained approximately  
3 \$297,000 in four forms of different digital currencies (bitcoin, litecoin, feathercoin, and worldcoin).

4 FORCE instructed CoinMKT to seize R.P.'s balances. CoinMKT effectuated this seizure by  
5 creating an entirely new account with the name "R\_seized."

6 On March 12, 2014, CoinMKT emailed FORCE, carbon copying others at the DEA, stating that  
7 it had created the "R\_seized" account, providing the login and password information and asking FORCE  
8 to "please advise when you would like us to move the funds" from the R.P. account into the R\_seized  
9 account. Later that same day FORCE replied to CoinMKT, including none of the other recipients on the  
10 original message in his reply, "Transfer them now please."

11 On March 23, 2014, using his official DEA email account with no one carbon copied, FORCE  
12 emailed CoinMKT noting that "we checked the balances this morning [in the R\_seized account] and the  
13 coins are still not there. Is everything okay?" CoinMKT replied later that same day that they had  
14 experienced some logistical issues in effectuating the transfer of digital currency from R.P.'s account to  
15 the R\_seized account.

16 On March 26, 2014, CoinMKT emailed FORCE stating "the [R.P.] funds should be in your  
17 account. We made the move 2 days ago but please confirm on your end that you have received them."  
18 FORCE replied, from his official DEA email account with no one carbon copied, "Yes they are in  
19 DEA's account now. Thank you very much!" I have confirmed that no such digital currency funds  
20 were received in any official DEA account, but instead went into FORCE's own personal account with  
21 Bitstamp, as described further below.

22 On April 3, 2014, FORCE emailed CoinMKT from his official DEA account, this time carbon  
23 copying three other DEA employees including his supervisor, directing CoinMKT to "please convert the  
24 \$37,051.08 that has been seized from R.P. into a certified check and forward it to DEA ... please make  
25 the certified check payable to the U.S. Marshals Service." CoinMKT did so and sent the government a  
26 certified check for \$37,051.08, representing that portion of R.P.'s account that had been in cash.

27 In a Report of Investigation dated March 11, 2014, FORCE wrote that "on March 13, 2014, DEA  
28 seized the following: 179.7977 bitcoin; 3,417.565 Litecoin; 366,511.2876 feathercoin; and

1 621,439,7182 worldcoin from [R.P.] for violations of the Bank Secrecy Act statutes, more specifically  
2 structuring financial transactions and money laundering. [R.P.] was exploiting CoinMKT to launder his  
3 illicit proceeds.” FORCE did not attempt to translate these various digital currency balances to any  
4 approximate dollar values as he had done in other instances. In a Report of Investigation dated April 3,  
5 2014, FORCE made reference to the earlier March 11 Report of Investigation and noted that “on April  
6 4, 2014, DEA seized \$37,206.30 from [R.P.] . . . FORCE directed CoinMKT to forward a certified check  
7 for \$37,206.30 to the U.S. Marshal’s Service.”

8 A Standard Seizure Form (SSF) is a government form that is typically completed by the DEA  
9 when funds are seized. FORCE prepared two SSFs relative to R.P.: (1) an SSF dated April 3, 2014, for  
10 the approximately \$37,000 in cash that was seized from R.P.’s account; and (2) an SSF dated March 12,  
11 2014, for the approximately \$297,000 worth of digital currency that was seized from R.P.’s account.  
12 However, FORCE instructed the DEA Asset Forfeiture Specialist not to input the digital currency SSF  
13 into the government’s computer tracking system for seized funds, the Consolidated Asset Tracking  
14 System (CATS), but rather to “hold” it for “a few months” or until further notice. The DEA Asset  
15 Forfeiture Specialist made a handwritten note on the digital currency SSF noting that FORCE had  
16 expressly directed it not be input at that time. FORCE included a copy of the SSF relating to the cash in  
17 the official case file of the Silk Road investigation.<sup>17</sup> However, he did not include a copy of the SSF  
18 relating to the digital currency in that same case file.

19 It appears that FORCE “papered up” the seizure of the digital currency portion of R.P.’s account  
20 in such a way that he may have thought he would be covered in the event anyone ever asked any  
21 questions about it being documented, but at the same time in a way that made it appear as if the  
22 approximately \$37,000 in cash was the sum total of all that was seized from R.P. Telling in this regard  
23 is that (1) when FORCE emailed from his official DEA account about the approximately \$37,000 in  
24 cash he carbon copied numerous individuals; the same was not true when he emailed about the  
25 approximately \$297,000 worth of digital currency; (2) FORCE’s co-case agent has advised that she was  
26

27 <sup>17</sup> My investigation confirmed with FORCE’s then-supervisor that the R.P. “case” had no known  
28 connection to the Silk Road.

1 of the belief that only approximately \$37,000 total was seized from R.P.'s account, and was unaware of  
2 the remaining approximately \$297,000 in digital currency that had been seized from R.P.'s account; (3)  
3 FORCE completed SSFs for both the cash and digital currency seizures but did not include the SSF for  
4 the digital currency in the case file; and (4) FORCE directed that the digital currency SSF be held.

5 In sum, I believe the way in which FORCE documented the R.P. seizure was FORCE's attempt  
6 to give himself plausible deniability by memorializing the digital currency seizure in both a Report of  
7 Investigation and SSF, albeit in a fashion that did not draw attention to the fact that it was worth  
8 approximately \$297,000. The documentation is particularly oblique for someone unfamiliar with digital  
9 currency, as many in FORCE's chain of command were.

10 The approximately \$297,000 worth of digital currency funds<sup>18</sup> from R.P.'s CoinMKT account did  
11 not make it to any official DEA or government account. Instead, that amount ultimately went into  
12 FORCE's personal Bitstamp account and was subsequently liquidated into U.S. dollars into FORCE's  
13 personal checking account. Specifically, on April 14, 2014, the funds moved from the R\_Seized  
14 account that CoinMKT had set up into a pass-through account. Then, on April 16, 2014, those funds  
15 moved from the pass-through account to FORCE's personal Bitstamp account. In late April 2014,  
16 FORCE made a withdrawal request of approximately \$201,000 from his Bitstamp account to his  
17 personal checking account. I have also confirmed with DEA that no case was ever opened against R.P.  
18 I am aware of no legal basis on which FORCE seized R.P.'s balances.

19 Within days of the seizure of the approximately \$297,000 in digital currency funds from R.P.,  
20 FORCE launched his own personal limited liability company dedicated to the investment in and  
21 speculation of digital currency, Engedi, LLC.

#### 22 **FORCE's Use of Official Subpoena for His Own Financial Gain**

23 Venmo is a payments platform company that enables person-to-person and merchant payment  
24 transactions using an application on mobile phones or other internet connected devices. Venmo is a  
25 subsidiary of PayPal, based in San Jose, California, and as discussed, relevant personnel from Venmo's  
26 compliance division are based in San Francisco, California, both within the Northern District of  
27

28 <sup>18</sup> The precise deposit amount was 222.9989 bitcoins.

1 California. On or about February 12, 2012, FORCE opened a Venmo account with the user name  
2 "cforce." That same day, a user by the name of "R.R." also opened a Venmo account.

3 Also on or about February 12, 2014, "R.R." initiated a payment to FORCE using Venmo's  
4 platform. The note on the transaction to FORCE stated: "Reversing payment #7163719 for \$2500.00  
5 from user [R.R.] to user better bitcoin." Venmo's fraud controls identified high risk payment activity  
6 and blocked both FORCE's and R.R.'s accounts.

7 On February 13, 2014, FORCE contacted Venmo by email from one of his personal email  
8 addresses to request, among other things, that his account with Venmo be unlocked so he could  
9 withdraw \$2,500. FORCE informed Venmo that R.R. was the target of a federal undercover  
10 investigation for which FORCE was the assigned case agent and the payment was for an undercover  
11 Bitcoin transaction. FORCE attached a copy of his badge and credentials in this email, and also  
12 mentioned in a post-script that he was interested in partnering with Venmo for employment  
13 opportunities.

14 On or about February 17, 2014, with his account at Venmo still blocked, FORCE served an  
15 administrative subpoena on Venmo from his official DOJ email account, Carl.M.Force@usdoj.gov, with  
16 a carbon copy to one of his personal email addresses. In this email, FORCE stated: "Please comply to  
17 the attached subpoena! If you should have any questions, please call me at 443.324.[XXXX]." The  
18 attached subpoena commanded the production of documents related to R.R. and directing Venmo's  
19 administrator to "lift the 'freeze' on the account of Carl Force, effective immediately." The subpoena  
20 itself contained a specific case matter number and grand jury number. FORCE sent this subpoena to  
21 Venmo's law enforcement contact within its compliance division, who was based in San Francisco,  
22 within the Northern District of California.

23 Given Venmo's belief that FORCE's request to unfreeze a personal account was not a proper use  
24 of an official government administrative subpoena, and given FORCE's repeated contact with Venmo  
25 from his personal email address, Venmo did not lift the freeze on FORCE's account and instead notified  
26 FORCE's superiors in the DEA. On February 24, 2014, FORCE emailed Venmo's compliance team in  
27 San Francisco and instructed them to disregard the subpoena.

1 On March 4, 2014, FORCE asked one of his co-case agents on the Baltimore Silk Road Task  
2 Force to run a query in a law enforcement database for Venmo, stating that he wanted to collaborate "on  
3 a suspicious money remitter, Venmo, Inc. Venmo has since registered with FinCEN, but I want to know  
4 if they have state money license remitting licenses in California and New York. Can you check? If not,  
5 I want to seize their bank accounts (need to identify them) á la BRIDGES and [M.M.'s] seizure warrants  
6 for Mt. Gox." In other words, FORCE appears to have been targeting Venmo for seizure after the  
7 company rebuffed his attempts to use a subpoena for his own personal matter.

8 On March 13, 2014, FORCE again used his personal email account to email Venmo's support  
9 division. In that email, FORCE advised Venmo that if they refused to unfreeze his account, he would  
10 retain an attorney and file a civil lawsuit. In another email FORCE sent to Venmo later that same day,  
11 FORCE explained the funds in his Venmo account were personal and stolen by R.R., and "As such, this  
12 \$2,500 has nothing to do with DEA, it was my personal assets that were stolen by [R.R.]" On March  
13 14, 2014, FORCE, again using his personal email address, directed Venmo not to contact the DEA  
14 again.

15 The administrative subpoena addressed to Venmo contains DEA Special Agent A.P.'s signature  
16 stamp on the signature line. A.P. was FORCE's acting supervisor during the relevant timeframe of the  
17 subpoena. A.P. stated he did not review or sign the subpoena and believes that FORCE, without A.P.'s  
18 knowledge, used A.P.'s signature stamp to execute the subpoena.

19 Following FORCE's submission of his letter of resignation on May 4, 2014, described above,  
20 another DEA employee witnessed FORCE taking boxes into a room where documents are taken to be  
21 permanently burned or destroyed. The contents of FORCE's burn boxes have since been seized and  
22 analyzed. Among other documents, these burn boxes contained copies of the administrative subpoena to  
23 Venmo. However, FORCE's superior reported that there are no copies of this subpoena in the Baltimore  
24 Silk Road case file.

25 Based on the foregoing, FORCE issued and used an official government subpoena for his own  
26 personal financial gain and transmitted it to a third party. By doing so, **there is probable cause to**  
27 **believe that FORCE committed a violation of the conflict of interest statute, in violation 18 U.S.C.**  
28 **Section 208.** I also believe FORCE was trying to cover up evidence of his use of the subpoena by

1 placing the copies in his burn box instead of the official case file. Furthermore, I believe that by  
2 directing Venmo to ignore the subpoena and not to contact the DEA, FORCE was attempting to obstruct  
3 justice by concealing his wrongful use of an official government subpoena for a personal matter.

4 **Additional Evidence Concerning Bitstamp**

5 Bitstamp is a global digital currency exchange headquartered in Europe with a limited U.S.  
6 presence in San Francisco, within the Northern District of California. On October 12, 2013, FORCE  
7 attempted to create an account with Bitstamp using identification documents in the name of his DEA-  
8 issued undercover identity. Bitstamp's verification process rejected these documents as not genuine.

9 FORCE thereafter provided Bitstamp with his own personal identification documents and his  
10 true and correct name, and Bitstamp created an account in FORCE's name. FORCE's Bitstamp account  
11 is associated with a single bank account and with two email personal addresses. One of the personal  
12 email addresses contains the moniker "fiat broker," which refers to someone who trades in currency.  
13 The account is associated with FORCE's personal checking account at M&T Bank.

14 On approximately November 9, 2013, FORCE made his first withdrawal request from Bitstamp  
15 for approximately \$34,000 worth of bitcoins.<sup>19</sup> I have reviewed FORCE's personal bank records and see  
16 an incoming international wire transfer to FORCE's bank account in the amount of approximately  
17 \$34,000 on November 13, 2013. Thereafter, FORCE made a second withdrawal request of Bitstamp for  
18 approximately \$96,000 worth of bitcoins. This withdrawal request triggered Bitstamp to conduct a  
19 Know Your Customer (KYC) check, also referred to as enhanced due diligence, on approximately  
20 November 20, 2013. This check essentially involved Bitstamp asking for more information from  
21 FORCE.

22 Throughout the latter part of November 2013, FORCE had a series of back and forth exchanges  
23 with Bitstamp using his personal email account. FORCE responded to Bitstamp's know-your-customer  
24 queries stating, among other things, the following: "I am a Special Agent with the Drug Enforcement  
25 Administration . . . and learned about Bitcoin through my investigation of SILK ROAD. I have attached  
26 a copy of my resume and a scanned copy of my badge and credentials."

27  
28 <sup>19</sup> All of these amounts represented in dollars from Bitstamp were in bitcoin based on their value  
at the time of the transfers.

1 It appears that FORCE's account with Bitstamp remained active after these initial know-your-  
2 customer checks, as his personal M&T bank records reveal two incoming deposits from his account with  
3 Bitstamp in January 2014 for approximately \$57,000 and \$50,000.

4 On April 18, 2014, FORCE requested a withdrawal from his account with Bitstamp of  
5 approximately \$80,000 to be deposited into his M&T bank account. Bitstamp flagged this request and  
6 conducted additional know-your-customer checks. Bitstamp's review showed that FORCE's account  
7 had been accessed using TOR. Given this, Bitstamp blocked FORCE's account.<sup>20</sup>

8 To unblock his account, FORCE made the following statements via an online support ticket with  
9 Bitstamp:

10 I am a U.S. Department of Justice – Drug Enforcement Administration (DEA), Special  
11 Agent who worked the original SILK ROAD website and corresponding investigation. I  
12 learned about Bitcoin through my investigation of DREAD PIRATE ROBERTS and  
13 SILK ROAD. I am attaching a scanned copy of my DEA credentials and badge to verify  
14 my status as Law Enforcement.

15 Again I obtained my bitcoin from investing a couple thousand dollars in the virtual  
16 currency in the beginning of 2012 when they were selling at \$4 a coin from exchanges  
17 such as GetBitcoin LLC (small "mom and pop" exchanges). Also, I have increased my  
18 holding of bitcoin through trading, the buying and selling, of the cryptocurrency.

19 I trade in Bitcoin. As such, I am constantly buying, shorting, selling, transferring,  
20 purchasing other assets such as real estate through RealtyShares and gold through  
21 goldsilverbitcoin.

22 I plan to continue to utilize Bitstamp to purchase and sell Bitcoin at a profit.

23 On April 24, 2014, as part of Bitstamp's fraud and theft prevention procedures, Bitstamp  
24 inquired why FORCE accessed his account through TOR and FORCE responded via the support ticket:

25 <sup>20</sup> Within a day after Bitstamp froze FORCE's account on April 18, 2014, FORCE sent an e-mail  
26 on April 19, 2014 to another DEA Special Agent whose primary responsibility was to account for  
27 undercover funds DEA had expended. FORCE's e-mail indicated that the Baltimore Silk Road Task  
28 Force had hundreds of bitcoin that they want to put into "service" and requested the creation of a DEA  
account with an exchange to liquidate bitcoin into U.S. dollars. That Special Agent advises that  
FORCE's April 19 e-mail was unusual because it was sent on a Saturday evening and there was a  
significant delay in time from when FORCE had acquired the bitcoin to when he sent the e-mail. I  
believe, based on my investigation, that the timing of FORCE's April 19 email was not coincidental  
given that Bitstamp had frozen his account earlier that day and he may have suspected that law  
enforcement had discovered that the bitcoins in his personal account were not his property. By sending  
such an e-mail, FORCE would be able to later maintain that he had tried to return the bitcoin to the  
government.

1 "I utilize TOR for privacy. Don't particularly want NSA looking over my shoulder :)" The following  
2 day, a member of Bitstamp's management learned of FORCE's comments and thought it was strange  
3 that a government official would make such a statement. FORCE's account was blocked again.

4 On April 28, 2014, FORCE made another withdrawal request from his account at Bitstamp of  
5 approximately \$201,000 worth of bitcoin to his personal bank account. It is clear that FORCE's account  
6 with Bitstamp was frozen and unfrozen numerous times during the April timeframe after FORCE  
7 verified his identity. After speaking with another then-member of federal law enforcement, BRIDGES,  
8 Bitstamp subsequently processed the withdrawal request, and FORCE's bank records reveal that he  
9 received approximately \$201,000 to his M&T bank account on May 6, 2014.

10 Based on my investigation described above, I believe that some if not all of the bitcoins that went  
11 into FORCE's account with Bitstamp was property that belonged to the government and/or third parties  
12 and that FORCE had come into possession of in his capacity as a DEA Special Agent, and not his own  
13 personally-acquired bitcoins, as he told Bitstamp.

14 On or about May 2, 2014, FORCE emailed Bitstamp to request that they delete all transaction  
15 history associated with his account. I believe, based on my investigation and the timing of FORCE's  
16 request, that this was an attempt by FORCE to conceal his activity.

#### 17 Evidence of FORCE's Improved Financial Picture

18 I have reviewed many but not all of FORCE's bank records from 2009 to present. I have also  
19 reviewed a financial analysis the FBI prepared of FORCE's financial history. Based on these sources,  
20 FORCE's financial situation and spending increased dramatically during 2013 and 2014, i.e., the  
21 timeframe of the wrongdoing described herein.

22 In summary, for the nearly two year period before FORCE worked the Silk Road case, FORCE  
23 deposited a total of approximately \$250,000 into his bank accounts, an amount consistent with his  
24 federal salary. In contrast to that, the bank records show that in the just over two-year timeframe from  
25 FORCE's joining the Silk Road case to his May 2014 resignation, FORCE deposited approximately  
26 \$776,000 into his bank accounts, an amount that represented solely his liquidation of bitcoins.

27 On or about February 17, 2012, FORCE began working on the Silk Road investigation.  
28 Thereafter, his financial situation improved markedly. In 2013 and 2014, FORCE had total deposits that



1 I have traced as bitcoin liquidation proceeds worth over approximately \$776,000. This includes, for  
2 example, six sizeable deposits into FORCE's checking accounts from his Bitstamp account totaling  
3 approximately \$518,000. There were also approximately \$118,000 worth of deposits from Coinbase,  
4 another San Francisco-based digital currency exchange company where FORCE had a personal account.

5 FORCE's spending also increased after his involvement on the Baltimore Silk Road Task Force.  
6 Aside from his approximately \$110,000 bitcoin investment into CoinMKT, FORCE paid off a \$22,000  
7 government loan on November 19, 2013. On December 2, 2013, he paid off his mortgage in full, which  
8 was approximately \$130,000 outstanding. On February 18, 2014, FORCE signed a "Purchaser  
9 Agreement" with RealtyShares, Inc., listing his net worth in excess of \$1 million, and providing a  
10 \$15,000 investment in three real properties.

11 On or about May 8, 2014, presumably after learning of the government's investigation and after  
12 he had resigned, FORCE wired \$235,000 to an offshore account in Panama. Records that I have  
13 recovered reveal that this wire was ultimately destined for BTC-e, a digital currency exchange outside  
14 the U.S. and that is not registered with the Department of the Treasury's Financial Crimes Enforcement  
15 Network ("FinCEN"). Based on evidence discussed further below, I believe that the vast majority – if  
16 not all – of this wire represented proceeds of illegal activities.

17 Other ways that FORCE appears to have spent some of the proceeds of his ultra vires activities  
18 include payments in the tens of thousands of dollars for the following:

- 19 • A June 2014 payment for the purchase of a company franchise;
- 20 • An August 2014 payment to a "Scottrade" account;
- 21 • A September 2014 transfer to an E\*Trade account;
- 22 • A September 2014 check payable to "Cash"

23 These are illustrative examples and not all of the financial outlays known to the government. Moreover,  
24 FORCE appears to have funded the business he opened on the side for speculating in Bitcoin, Engedi,  
25 LLC, with money from his personal checking accounts into which he had transferred ill-gotten proceeds.  
26 On May 7, 2014, FORCE opened a new bank account with Gardner Bank in the Engedi, LLC name,  
27 funding it 20 days later with an \$8,000 check from FORCE's personal M&T checking account. And on

28

1 July 28, 2014, FORCE transferred \$93,000 from his personal M&T checking account to the Engedi  
2 account at Gardner Bank.

3 **FORCE's False Statements and Obstructive Conduct**

4 Upon learning he was the subject of this investigation, FORCE, through counsel, approached the  
5 government about meeting for a voluntary interview. FORCE signed the Northern District of California  
6 and Public Integrity Section's standard form Proffer Agreement, sometimes known as a "Queen for a  
7 Day" letter. This Agreement is standard in criminal investigations and provided, among other things,  
8 that if FORCE was truthful, the government could not make direct use of the information FORCE  
9 provided against him in a future case-in-chief. An important exception to the protections of the Proffer  
10 Agreement was that FORCE could be prosecuted for perjury, obstruction of justice, or false statements  
11 in the event he was untruthful during the session.

12 Pursuant to the Proffer Agreement, FORCE met with representatives from the U.S. Attorney's  
13 Office for the Northern District of California, the Public Integrity Section, the FBI, IRS, and DOJ OIG,  
14 on May 30, 2014. During that proffer session, FORCE was specifically asked whether he had ever used  
15 the moniker "French Maid." FORCE denied that he had. As demonstrated above, this was not truthful  
16 as FORCE had operated as "French Maid" in communications with DPR, among other personas.

17 Additionally, FORCE's conduct throughout the investigation obstructed the real proper purpose  
18 of the Baltimore Silk Road Task Force which was to identify, locate and arrest DPR and other Silk Road  
19 users. At numerous points, FORCE corruptly obstructed the lawful investigation into DPR and Silk  
20 Road by pursuing his own personal and unlawful goals.

21 **VIII. BRIDGES PROBABLE CAUSE**

22 **Bridges' Background**

23 Former Secret Service Special Agent BRIDGES was also on the Baltimore Silk Road Task Force  
24 and worked alongside FORCE. Until March 18, 2015, before he abruptly resigned, BRIDGES had been  
25 assigned to the Secret Service's Electronic Crimes Task Force. His specialty was in computer forensics  
26 and anonymity software derived from TOR. Another member of the Baltimore Silk Road Task Force  
27 that has been interviewed confirmed that BRIDGES was the Task Force's subject matter expert in  
28 Bitcoin.

1 In these roles, BRIDGES had access to and used digital currency and was the affiant on various  
2 seizure warrants pertaining to digital currency. In fact, on May 9, 2013, BRIDGES was the affiant on  
3 one of the largest-ever seizures from a digital currency exchange. This was an approximately \$2.1  
4 million seizure pertaining to the digital currency exchange Mt. Gox, purportedly because Mt. Gox had  
5 violated 18 U.S.C. Section 1960 by failing to register with the Financial Crimes Enforcement Network  
6 (FinCEN) and thus was engaged in operating an unlicensed money service business. This is not the only  
7 matter on which BRIDGES served as the affiant.

### 8 The Silk Road Theft and BRIDGES' Fidelity Account

9 C.G. was one of DPR's employees and functioned as a Silk Road customer support  
10 representative, under the username "Flush." In this role, C.G. had administrator access to the Silk Road  
11 website,<sup>21</sup> meaning C.G. had certain administrative privileges on the Silk Road website, including the  
12 ability to access vendor accounts and reset Silk Road user and vendor passwords and pins.

13 On or about January 17, 2013, FORCE and BRIDGES were part of a team that apprehended  
14 C.G. in a controlled delivery for a kilogram of cocaine. C.G. was arrested and soon thereafter began to  
15 cooperate with law enforcement, turning over his Silk Road login credentials in the process to members  
16 of the Baltimore Silk Road Task Force. During this same timeframe C.G. also turned over access to his  
17 account and passwords to other digital currency accounts to include his Mt. Gox and Dwolla accounts.  
18 As a result of this controlled delivery, C.G. was charged with federal criminal narcotics charges.<sup>22</sup>

19 One of the accounts that C.G. provided access to was a Silk Road administrator account named  
20 "Flush." C.G. acted as a Customer Service representative on the Silk Road site using the account name  
21 "Flush." But on January 17, 2013, C.G. turned over access to the "Flush" account to members of the  
22 Baltimore Silk Road Task Force. C.G. also executed several consent forms authorizing law enforcement  
23 to use and assume the "Flush" identity.<sup>23</sup>

24  
25 <sup>21</sup> This should not be construed as someone who had root access to the server.

26 <sup>22</sup> It should be noted that C.G. is cooperating with law enforcement and is hoping for leniency in  
27 sentencing as a part of his cooperation. C.G.'s criminal history includes convictions for filing a  
28 fraudulent insurance claim and acquiring a controlled substance by prescription alteration.

<sup>23</sup> Because of concerns about C.G.'s whereabouts, DPR at some point cut off the "Flush"  
account's access, but through communications with DPR, C.G. was able to regain access to the account  
on January 20, 2013, and pass that information onto the Baltimore Silk Road Task Force.

1 On January 25, 2013, C.G. debriefed with FORCE, BRIDGES, and other members of the  
2 Baltimore Silk Road Task Force. According to BRIDGES' report of the interview, C.G. showed them  
3 how to log into Silk Road vendor accounts and reset passwords, how to change the status of a seller to a  
4 vendor, how to reset pins, and information about how the Silk Road administrative functions worked.  
5 BRIDGES' text messages indicate that he left the proffer session after one day, and a Silk Road Task  
6 Force member stated that BRIDGES told him that he left the latter part of the January 25, 2013,  
7 proffer.<sup>24</sup>

8 On January 25, 2013, during the afternoon and into the night, the Silk Road website suffered a  
9 series of sizeable thefts. These thefts affected certain Silk Road vendors and overlapped with the time of  
10 the C.G. proffer session. The thefts were accomplished through a series of vendor password and pin  
11 resets, something that could be accomplished with the administrator access that C.G. had given to the  
12 Baltimore Silk Road Task Force.

13 On January 26, 2013, the proffer of C.G. continued. BRIDGES left early and did not participate  
14 on this day. At some point during that day, DPR communicated to Nob (FORCE) that Silk Road had  
15 suffered thefts and that those thefts were associated with C.G.'s account. Law enforcement questioned  
16 C.G. about this, and C.G. denied that he had committed the thefts. According to chats I have reviewed  
17 from the Silk Road servers and from Ulbricht's laptop (as well as communications between DPR and  
18 one of his employees at the time of the January 25, 2013 thefts) it appears that DPR and the employee  
19 believed C.G. was responsible for the thefts, because they managed to associate C.G.'s account, "Flush,"  
20 with the theft.<sup>25</sup> As a result of DPR's belief that C.G. was responsible for the thefts, DPR communicated  
21 with Nob (FORCE) – whom he believed to be a major drug dealer with the ability to procure hit men –  
22 and hired Nob to have his associates kill C.G. DPR also communicated with another individual and  
23 commissioned a hit on C.G. For the hit that Nob's associates were to perform, DPR paid Nob a total of  
24 approximately \$80,000 through a bank wire transfer for the murder. FORCE and C.G., together with  
25 assistance from others on the Baltimore Silk Road Task Force, then faked C.G.'s death to make it look

26 \_\_\_\_\_  
27 <sup>24</sup> This Task Force member was not present for the C.G. debrief but indicated that BRIDGES had  
told him this information.

28 <sup>25</sup> On or about January 26, 2013, according to chats between DPR and another employee,  
"Flush's" administrative account was shut down in order to prevent further theft.

1 as if Nob's associates had killed C.G. BRIDGES was to assist with perpetrating this supposed murder-  
2 for-hire by working on "proof of death" photographs of C.G. that Nob (FORCE) was to send to DPR.

3 Based on my review of the data from the Silk Road servers, I believe the initial Silk Road thefts  
4 were likely committed by whoever was controlling a Silk Road account with the username "Number13."  
5 Prior to January 25, 2013, "Number13" had been an ordinary buyer account on Silk Road. On January  
6 25, 2013, however, "Number13" was given vendor privileges. Also on January 25, 2013, the "Flush"  
7 account made a transfer of approximately 900 bitcoins into account "Number13." This appears to have  
8 been the first of multiple thefts that occurred that day from the Silk Road website.

9 My analysis of both the block chain and data recovered from the Silk Road servers reveals that,  
10 also on January 25, 2013, a single Bitcoin address received no less than 20,000 bitcoins.<sup>26</sup> The first  
11 transaction into that Bitcoin address was a deposit by account "Number13." These transactions are  
12 demonstrated on the attached Exhibit F ("Liquidation of Silk Road Theft Proceeds").

13 I believe that BRIDGES controlled and/or had access with others to "Number13," the account  
14 that appears to have initiated the sizeable bitcoin thefts. I believe this for at least two reasons. First, in a  
15 DEA 6 that FORCE authored dated January 23, 2013, FORCE described how he had transferred 60  
16 bitcoins into a DEA-controlled account known as "TrustUsJones." Data from the Silk Road servers  
17 demonstrates that on that January 23, 2013 date, there was a 60 bitcoin transfer from "Number13" into  
18 "TrustUsJones." Second, in an email dated January 23, 2013, FORCE emailed BRIDGES requesting  
19 that BRIDGES deposit bitcoins to replenish the "TrustUsJones" account. In other words, BRIDGES, in  
20 consultation with FORCE, appears to have been controlling "Number13" during the late January 2013  
21 timeframe.

22 On January 26, 2013, my analysis of the block chain reveals that at least 2,430 of the bitcoins  
23 stolen from the Silk Road went into another single Bitcoin wallet address. These transactions are also  
24 depicted on the attached Exhibit F. I have conferred with an individual who has a substantial  
25

26 <sup>26</sup> I believe that the aggregate total of the thefts was approximately 20,000 bitcoin. The dollar  
27 value of 20,000 bitcoin would have varied dramatically depending on when the value was calculated due  
28 to the fluctuating value of bitcoin. At the time of thefts in January 2013, 20,000 bitcoin would have  
been worth approximately \$350,000. At its peak price, however, it would have been worth far more, in  
excess of approximately \$20 million.

1 background in block chain analysis who advised me that this wallet funded a Mt. Gox exchange account  
2 totaling 2,430 bitcoins. As noted, Mt. Gox was the world's largest digital currency exchange based in  
3 Japan.

4 Chats I have reviewed between DPR and one of his employees indicate that DPR and the  
5 employee launched an internal investigation into who was responsible for the January 25, 2013 theft.  
6 Those chats reveal that DPR's own internal investigation initially led him to account "Number13" as  
7 being associated with the thefts. Chats further reveal that "Number13" sent DPR a chat on January 27,  
8 2013 saying "Whats [sic] going on . . . I really need that money back. What has happened to all my  
9 BC? Within the past day someone withdrawled [sic]<sup>27</sup> all my bc from my account without my  
10 permission. The fact they must have had a pin really confuses me and makes me think it was something  
11 on your end." This caused DPR to reply to "Number13" stating "Your account is under investigation  
12 I'm afraid. What is your relationship with the user [omitted]?" During a back and forth between the  
13 two, "Number13" wrote, "I don't know what any of that other crap in my history is. Look at my history,  
14 I am a buyer not a seller. What is going on man?" This caused DPR to reply, "You're all set, sorry for  
15 the trouble." DPR was physically present in San Francisco on the date of these communications with  
16 "Number13."

17 The Silk Road thefts were completed on January 25, 2013. Within days, BRIDGES began to  
18 text FORCE asking that FORCE (as Nob) get advice from DPR about liquidating bitcoins into dollars.  
19 For example, on January 30, 2013, BRIDGES texted FORCE: "Next time you chat with DPR do you  
20 think he would touch on the topic of how he moves bitcoins, meaning what exchange he uses? He  
21 should have some advise [sic] if you will be doing big drug deals on how to exchange all that back into  
22 US dollars." FORCE replied that he had asked DPR that before and DPR would not provide an answer.  
23 BRIDGES replied, "Roger. Just curious."

24 Approximately two weeks after the Silk Road thefts, on February 12, 2013, BRIDGES formed  
25 "Quantum International Investments, LLC," (Quantum) and registered it with the Maryland Secretary of  
26

27 \_\_\_\_\_  
28 <sup>27</sup> The individual controlling "Number13" on this date spelled withdrawal as "withdrawled."  
When BRIDGES texted FORCE on February 23, 2013, as discussed herein, BRIDGES also spelled the  
word withdrawal incorrectly using the slightly different "withdrawlaed."

1 State. On February 22, 2013, BRIDGES established a personal investment account at Fidelity in the  
2 Quantum name. That account was associated with BRIDGES' Social Security number and other  
3 accounts in BRIDGES' name. That day and the next, BRIDGES began to text with FORCE about  
4 getting C.G.'s help and transferring bitcoins. Specifically, BRIDGES texted FORCE on February 22,  
5 2013: "Whenever you are working next can we talk. [The prosecutor] said you have the gift of  
6 convincing [C.G.] to do things and we need you to convince him to do something. Whenever your [sic]  
7 available can we chat." Then on February 23, 2013, BRIDGES texted FORCE: "Need your help with  
8 DPR if you can. I am trying to transfer out our USSS Bitcoins and they have not shown up in over 30  
9 hours after being withdrawlaed [sic]. Can you hit up DPR and say one of your workers or financial guys  
10 bitcoins are not showing up? I am going to get my butt kicked if this money is missing. After 30 hours  
11 I am getting really concerned. Our one UC account is '[omitted name]' Can you use your raport [sic]  
12 and help me out? I did the transfer yesterday morning."

13 It is clear that during this time period both BRIDGES and FORCE were actively monitoring the  
14 price of bitcoin. On February 24, 2013, BRIDGES texted FORCE, "If you got bitcoins on SR [Silk  
15 Road] get them off...." By the end of March, BRIDGES and FORCE were texting about the value of  
16 bitcoin. On March 20, 2013, FORCE texted BRIDGES "Bitcoin just hit \$63 . . . what the slip [sic]?" to  
17 which BRIDGES replied "Ya!" and then FORCE replied, "[sp]eculation about big investors going in  
18 later this month. Along with the demand is exceeding supply." Then on March 21, 2013, BRIDGES  
19 texted FORCE "75 dollars now" and FORCE replied "Geez."

20 I have obtained and reviewed Fidelity records for BRIDGES' Quantum account. Those records  
21 demonstrate that between March 6, 2013 and May 7, 2013, the account received nine separate wire  
22 transfers originating from Mt. Gox in Japan. The wires totaled in excess of \$820,000, and were each  
23 less than \$100,000. Fidelity has confirmed that BRIDGES' Quantum account was funded solely by  
24 deposits from Mt. Gox and no other source.

25 The final wire from Mt. Gox to BRIDGES' Quantum account was on May 7, 2013. Just two  
26 days later, BRIDGES served as the affiant on a seizure warrant for \$2.1 million in Mt. Gox accounts. I  
27 know from my training and experience as a law enforcement officer that the process of putting together  
28 an affidavit in support of a warrant is time consuming and often takes several days, if not longer, to

1 prepare. In serving as an affiant for Mt. Gox bank accounts a mere two days after he had personally  
2 received a wire from Mt. Gox (the latest in a series of wires), BRIDGES had a conflict of interest.

3 In early 2015, by which time BRIDGES knew of the Northern District of California's  
4 investigation into the Baltimore Silk Road Task Force, BRIDGES was working on an unrelated  
5 investigation. Under the guise of that other investigation, BRIDGES contacted Coinbase, a digital  
6 currency exchange based in San Francisco. However, instead of asking only questions concerning the  
7 other investigation, Coinbase representatives report that BRIDGES engaged them in a series of  
8 questions about whether and how Mt. Gox accounts could be traced. Coinbase found this odd, given  
9 that the stated purpose of BRIDGES' calls concerned an unrelated investigation.

10 Based on the foregoing, I believe that BRIDGES, or someone acting on his behalf, utilized the  
11 "Flush" and "Number13" accounts, but particularly the "Flush" account to fraudulently act as an  
12 administrator to reset pins and passwords on various Silk Road vendors' accounts, and then caused  
13 bitcoins to be moved from those accounts into a particular wallet and then into the Mt. Gox exchange.  
14 Moreover, I believe that BRIDGES, and/or someone working with him or acting on his behalf, used the  
15 "Number13" account to communicate with DPR and fraudulently represent that "Number13" was a  
16 buyer account on Silk Road who had nothing to do with the theft to stave off DPR's investigation into  
17 "Number13" and its activity. I believe these communications were material. At the time of these  
18 communications, DPR was in the Northern District of California, and the Bitcoin stolen as a result of the  
19 Silk Road thefts was in a Bitcoin address and had not yet been transferred to Mt. Gox. For all of these  
20 reasons, **there is probable cause to believe that BRIDGES committed wire fraud, in violation of 18**  
21 **U.S.C. Section 1343.**

#### 22 **BRIDGES' Conduct During The Investigation**

23 On April 29, 2014, Bitstamp's General Counsel advised BRIDGES by telephone from the  
24 Northern District of California that Bitstamp suspected FORCE of wrongdoing and intended to formally  
25 bring it to the attention of law enforcement via a Bank Secrecy Act filing. Bitstamp did so on May 1,  
26 2014. By May 4, 2014, FORCE submitted a letter of resignation after 15 years of service to be effective  
27 later that month.



1 On approximately May 2, 2014, the U.S. Attorney's Office for the Northern District of  
2 California opened an official investigation into FORCE concerning his activities with his Bitstamp  
3 account and bitcoin holdings. On approximately May 4, 2014, the Public Integrity Section opened an  
4 official investigation into FORCE concerning his improper use of a subpoena to Venmo. On May 8,  
5 2014, the Northern District of California and Public Integrity investigations were merged.

6 Between April 29, 2014 and May 5, 2014, an analyst with whom BRIDGES worked at the Secret  
7 Service, E.P., ran several queries in a government database looking for Bank Secrecy Act filings on both  
8 FORCE and BRIDGES. That analyst later ran another query on BRIDGES on or about June 27, 2014,  
9 this time using BRIDGES' Social Security number. I know from my training and experience that access  
10 to certain government databases is restricted and may not be used for personal matters. Based on my  
11 investigation, I believe that BRIDGES may have directed the analyst to conduct these queries because  
12 he was worried that a financial institution may have made a Bank Secrecy Act filing on him given the  
13 multiple transfers from Japan into his Quantum Fidelity account.<sup>28</sup>

14 On May 28, 2014, BRIDGES was telephonically interviewed by a Special Agent with the FBI's  
15 Public Corruption Squad in San Francisco, as part of the Northern District of California's investigation.  
16 BRIDGES was joined by an attorney representing him and also by a high-level superior from the U.S.  
17 Secret Service. BRIDGES was advised of the nature of the interview and of the identity of the  
18 interviewer. During that interview, BRIDGES stated that although he knew FORCE through their work  
19 on the Baltimore Silk Road Task Force, they had minimal contact, and BRIDGES had no knowledge of  
20 any of FORCE's activity related to the purchase of bitcoins. BRIDGES added that FORCE was  
21 unprofessional and that after learning of the Bank Secrecy Act filing of which FORCE was a subject,  
22 BRIDGES briefed the most senior manager in his office, the Special Agent in Charge (SAC) of the  
23 Baltimore Field Office. The SAC told BRIDGES not to discuss the matter with anyone. BRIDGES  
24 specifically denied during the May 28, 2014, interview that he ever told FORCE about the Bank Secrecy  
25 Act filing. He also denied having owned any Bitcoin in over a year.

26  
27  
28 <sup>28</sup> I believe that the analyst, E.P., ultimately confirmed that she ran BRIDGES in the database,  
but essentially stated that she could not remember whether BRIDGES had specifically asked her to do  
so. E.P. had BRIDGES' Social Security number for the second query she ran.

1 On November 13, 2014, BRIDGES was again interviewed as part of the Northern District of  
2 California's investigation, this time by representatives from the Justice Department's Public Integrity  
3 Section and Office of the Inspector General. BRIDGES was advised of the nature of the interview and  
4 of the identity of the interviewers. BRIDGES advised he had been an affiant on a \$2.1 million seizure  
5 of accounts belonging to Mt. Gox, a digital currency exchange. He described himself as a subject matter  
6 expert on TOR, and stated that other members of the Silk Road Task Force would routinely consult him  
7 on security and undercover-type questions associated with ongoing Silk Road investigations. During  
8 this interview he reiterated what he had told the FBI Special Agent previously on May 28, 2014, namely  
9 that he and FORCE did not have a close working relationship. When questioned about Quantum  
10 International Investments, LLC, BRIDGES acknowledged that he created the LLC as a personal  
11 business venture, but stated that he had requested and obtained specific approval from the Secret Service  
12 Office of General Counsel (OGC) to establish the LLC and use it for investment purposes.

13 In contrast to what BRIDGES stated during these interviews, my investigation has revealed that  
14 several of BRIDGES' statements were not accurate. These statements were capable of and did influence  
15 the government's investigation.

16 On March 18, 2015, BRIDGES resigned after being told he was being suspended. USSS  
17 personnel advised BRIDGES to leave behind his two government-issued computers in the evidence  
18 vault. Although he properly tendered one computer where directed, he placed a second Apple brand  
19 laptop computer in a cabinet directly above an area that USSS Baltimore personnel use as a "wipe"  
20 station.<sup>29</sup> I do not believe BRIDGES would have any reason to store the laptop in this area, other than  
21 for it to be in close proximity to computers to be wiped, as USSS personnel has advised this is not a  
22 storage area for laptops. Moreover, after BRIDGES was advised of his suspension, he asked his  
23 supervisor if he could access his Dell laptop computer to copy electronic receipts of personal items he  
24 had purchased from internet merchants. However, instead of copying receipts, BRIDGES began  
25 copying a folder entitled "Bitstamp." Upon noticing what BRIDGES was copying, his supervisor  
26 secured the laptop and did not allow BRIDGES further access.

27  
28 <sup>29</sup> Computers were left in the "wipe" station for the purpose of having their hard drives permanently erased.

1 **BRIDGES' Money Laundering**

2 On June 2, 2014, just days after being interviewed by the FBI Special Agent in this matter,  
3 BRIDGES wired approximately \$225,000 in criminal proceeds from his Fidelity Quantum account to an  
4 account at PNC Bank. He later wired another approximately \$30,000 from the Fidelity Quantum  
5 account to the PNC account on or about July 7, 2014. The PNC account was in the name of a third-  
6 party with whom BRIDGES had a personal relationship, and BRIDGES' name was also on the account.  
7 As described above, BRIDGES' Quantum Fidelity only contained funds transferred from Mt. Gox, and  
8 based on the evidence described in the "Silk Road Theft" section above, I believe the Mt. Gox transfers  
9 represented criminal proceeds. Given that BRIDGES wired \$225,000 in criminal proceeds from his  
10 Quantum Fidelity account (representing proceeds of wire fraud, a specified unlawful activity) into a  
11 different account in the name of a third-party at another financial institution just days after being  
12 questioned in this matter, I believe that BRIDGES was attempting to conceal the source and nature of  
13 the proceeds and further impede the investigation. Given the foregoing, **there is probable cause to**  
14 **believe that BRIDGES' \$225,000 wire constituted money laundering in violation of 18 U.S.C.**  
15 **§ 1956.**

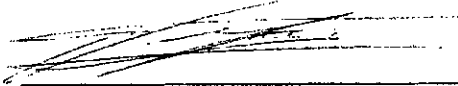
16 **CONCLUSION**

17 Based on my training and experience and the facts as set forth in this affidavit, there is probable  
18 cause to believe that FORCE has committed violations of law to include Title 18, United States Code,  
19 Section 641 (Theft of Government Property), Title 18, United States Code, Section 1343 (Wire Fraud),  
20 and Title 18, United States Code, Section 1956 (Money Laundering), and Title 18, United States Code,  
21 Section 208 (Conflict of Interest). There is also probable cause to believe that BRIDGES has committed  
22 violations of law to include Title 18, United States Code, Section 1343 (Wire Fraud) and Title 18,  
23 United States Code, Section 1956 (Money Laundering). I therefore request that you issue the attached  
24 arrest warrants and criminal complaint.

**REQUEST FOR SEALING**

I further request that the Court order that all papers in support of this affidavit, including the affidavit and criminal complaint, be sealed until further order of the Court or until the apprehension and/or surrender of the subjects, whichever is earlier. These documents discuss an ongoing criminal investigation that is neither public nor known to all involved in the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may jeopardize that investigation by alerting the subjects in advance of apprehension and/or surrender. In addition, for the reasons stated in the attached Paragraph meant for inclusion at Page 11 of the Affidavit, I request that that Paragraph be sealed until further Order of this Court. The government will move to unseal that Paragraph as soon as practicable, as detailed in the sealed portion of that Paragraph attached. A Proposed Order is attached.

Respectfully submitted,

  
TIGRAN GAMBARYAN  
Special Agent  
Internal Revenue Service

Subscribed and sworn to before me on this 25<sup>th</sup> day of March, 2015

  
HONORABLE MARIA-ELENA JAMES  
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND

RECEIVED  
U.S. DISTRICT COURT  
DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

vs.

CARL MARK FORCE

\*  
\*  
\*

2015 MAR 30 P 2:22

Case No. 15-0656TJS


\*\*\*\*\*

ORDER OF TEMPORARY DETENTION PENDING HEARING  
PURSUANT TO BAIL REFORM ACT

Upon motion of the United States for Temporary Detention, it is ORDERED that a detention hearing is set for April 2 2015 (date) at 9:30 (time) before Hon. Timothy J. Sullivan, United States Magistrate Judge, 101 West Lombard Street, Baltimore, Maryland 21201 Courtroom 7B.

Pending this hearing, the defendant shall be held in custody by (the United States Marshal) ( \_\_\_\_\_ ) (Other Custodial Official) and produced for the hearing.

March 30, 2015  
Date

  
\_\_\_\_\_  
Timothy J. Sullivan  
United States Magistrate Judge

FILED \_\_\_\_\_ ENTERED \_\_\_\_\_  
LODGED \_\_\_\_\_ RECEIVED \_\_\_\_\_

MAR 30 2015

AT BALTIMORE  
CLERK U.S. DISTRICT COURT  
DISTRICT OF MARYLAND

BY

DEPUTY

