EXHIBIT 5

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

ROSS ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

AFFIDAVIT IN SUPPORT OF GOVERNMENT'S FORFEITURE MOTION

S1 14 Cr. 68 (LGS)

STATE OF NEW YORK)
COUNTY OF NEW YORK) ss.:
SOUTHERN DISTRICT OF NEW YORK)

Trevor McAleenan, Special Agent, Internal Revenue Service – Criminal Investigation Division ("IRS-CI"), being duly sworn, deposes and says:

I. Introduction

1. I am a Special Agent of the IRS-CI, and I have been employed in this position for over eight years. During that time, I have participated in investigations of wire fraud, cyber-thefts and misappropriations, computer hacking, and money laundering, including thefts from dark-web internet marketplaces and fraudulent schemes involving cryptocurrency, and am familiar with various means and methods used to commit such offenses.

2. This affidavit is submitted in support of the United States of America's application, pursuant to Rule 32.2(e) of the Federal Rules of Criminal Procedure, for an Amended Preliminary Order of Forfeiture relating to subsequently located property, in which the Government seeks the forfeiture of 51,351.89785803 Bitcoin ("BTC") (the "Subsequently Located Silk Road BTC"), which are certain specific assets that, as the district court found at sentencing, were involved in

and/or are traceable to defendant Ross Ulbricht's laundering of criminal proceeds, as set forth in more detail below.

3. This affidavit is based on, among other sources of information: (i) my personal knowledge; (ii) information provided to me by other law enforcement officers at IRS-CI and the United States Attorney's Office for the Southern District of New York participating in the investigation described herein; (iii) public documents from *United States v. Ulbricht*, S1 14 Cr. 68, including the trial transcript and exhibits, Presentence Investigation Report dated April 28, 2015 ("PSR"), May 29, 2015 Sentencing Transcript ("Sentencing Tr."), and preliminary order of forfeiture/money judgment; (iv) prior search warrants and affidavits related to the Silk Road; (v) various forensic analyses of computer servers used to operate the Silk Road dark-web internet marketplace; (vi) public information contained in the Bitcoin blockchain; (vii) my participation in a November 9, 2021 judicially authorized premises search warrant and my review of items seized that day and subsequently provided to the Government by the occupant of the premises; (viii) the review and analysis of various records from banks, credit card companies, cryptocurrency exchanges, message boards, internet service providers, a blockchain tracing provider, and e-commerce merchants; (ix) the guilty plea allocution that occurred on November 4, 2022 and accompanying plea agreement in *United States v. Zhong*, 22 Cr. 606 (PGG) (S.D.N.Y.); and (x) my training and experience. This affidavit does not include all the facts that I have learned during the course of this investigation. Where dates, figures, and calculations are set forth herein, they are approximate. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

II. Background on Silk Road

4. In the course of this investigation, I have gained extensive familiarity with the Silk

Road dark-web internet marketplace through various means, including by reviewing public documents from *United States v. Ulbricht*, S1 14 Cr. 68, including the trial transcript and exhibits, PSR, sentencing transcript, and preliminary order of forfeiture/money judgment; reviewing prior search warrants and affidavits related to Silk Road; discussing Silk Road's operation with other law enforcement agents; and reviewing the results of various forensic analyses of computer servers used to operate the Silk Road dark-web internet marketplace.

5. Silk Road was an online "darknet" black market. In operation from approximately 2011 until 2013, Silk Road was used by numerous drug dealers and other unlawful vendors to distribute massive quantities of illegal drugs and other illicit goods and services to many buyers, and to launder all funds passing through Silk Road.

6. For his role in creating and operating the Silk Road dark-web internet marketplace, following a jury trial in the Southern District of New York, Ulbricht ultimately was convicted on various charges, including charges relating to distributing narcotics by means of the internet, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents, and conspiring to commit money laundering. Ulbricht was sentenced to life in prison. *See United States v. Ulbricht*, S1 14 Cr. 68.

7. Based on my familiarity with the Silk Road dark-web internet marketplace, *see supra* ¶ 4, I learned the following about the illegal nature of the goods and services sold on the site:

a. The illegal nature of the items sold on Silk Road was readily apparent to any user browsing through its offerings. The vast majority of the goods for sale consisted of illegal drugs of nearly every variety, which were openly advertised on the site as such and were immediately and prominently visible on the site's home page. The offerings for sale on the site at

any single time amounted to multi-kilogram quantities of heroin, cocaine, and methamphetamine, as well as distribution quantities of other controlled substances, such as LSD.

b. In addition to illegal narcotics, other illicit goods and services were openly sold on Silk Road as well. These included, for example, illegal computer hacking services, malicious software (such as password-stealing programs), forged identity documents, stolen financial and/or identity information, and murder-for-hire or "hitman" services.

c. The Silk Road forum also contained extensive guidance on how to evade law enforcement. The Silk Road forum included, for instance, numerous postings by users offering advice to other users on how they should configure their computers so as to avoid leaving any trace on their computer systems of their activity on Silk Road.

8. Based on my familiarity with the Silk Road dark-web internet marketplace, I learned the following concerning the payment system used to process purchases made through the site:

a. The only form of payment accepted on Silk Road was a form of digital currency (also called cryptocurrency) known as Bitcoin.

b. Silk Road's payment system essentially consisted of a Bitcoin "bank" internal to the marketplace, where every user had to hold an account in order to conduct transactions on Silk Road. Specifically, every Silk Road user had at least one Silk Road Bitcoin address associated with the user's Silk Road account. These addresses were stored on wallets maintained on servers controlled by Silk Road.

c. In order to make purchases on the Silk Road marketplace, the user first had to obtain Bitcoin and send them to a Bitcoin address associated with the user's Silk Road account.

d. After funding the user's account, that user could then make purchases from Silk Road vendors. When the user purchased an item on Silk Road, the Bitcoin needed for the purchase were held in escrow by Silk Road pending completion of the transaction.

e. The user's Bitcoin were then transferred to the Silk Road Bitcoin address of the vendor involved in the transaction. The vendor could then withdraw Bitcoin from the vendor's Silk Road Bitcoin address by requesting that Silk Road withdraw the Bitcoin to a different Bitcoin address, outside of Silk Road, such as the address of a Bitcoin exchange, which Silk Road would then process. That exchange could then, upon the vendor's request, exchange the Bitcoin for fiat currency or an alternative form of digital currency.

f. Silk Road charged a commission for every purchase conducted by its users. The commission rate varied, generally between 8 to 15 percent per transaction, depending on the size of the sale: the larger the sale, the lower the commission.

g. Ulbricht carefully conceived of Silk Road's business model to facilitate anonymous illegal transactions beyond the reach of law enforcement, including by hosting the site on the Tor network, which hides the identities of its users and their IP addresses, and by requiring vendors and customers to do business in Bitcoin, a virtual currency designed to be as anonymous as cash.

h. Further, during its operation, Silk Road made use of a so-called "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Bitcoin blockchain. As described in the Silk Road "wiki" page, Silk Road's tumbler sent "payments through a complex, semi-random series of dummy transactions . . .making it nearly impossible to link your payment with any coins leaving the site." PSR ¶ 41. In other words, if a buyer made a payment on Silk Road, the tumbler obscured any link between the buyer's Bitcoin address and the vendor's Bitcoin address where the Bitcoin ended up.

By Ulbricht's design, this made it challenging to use the Bitcoin blockchain to follow the money trail involved in a given transaction, even where the buyer and vendor Bitcoin addresses were both known. Based on my training and experience, an important and common function served by such "tumblers" is to assist with the laundering of criminal proceeds.

9. During the course of the Silk Road investigation, law enforcement located a number of computer servers associated with the operation of Silk Road. The FBI seized computer servers located in Iceland and the United States that were used to operate and back up Silk Road (the "Silk Road Servers"). PSR ¶ 59. IRS-CI obtained images of the Silk Road Servers. The Silk Road Servers include computer databases which contained records for transactions which occurred on Silk Road during the course of its operation. The transactional database included detailed information regarding each transaction, including the category of product that was sold, the purchase price, both in Bitcoin and in U.S. dollars, and the commission taken by Silk Road, also in both Bitcoin and U.S. dollars. PSR ¶ 59.

10. From reviewing public documents from *United States v. Ulbricht*, S1 14 Cr. 68, including the trial transcript and exhibits, PSR, sentencing transcript, and preliminary order of forfeiture/money judgment, prior search warrants and affidavits related to Silk Road, as well as the results of IRS-CI forensic reviews performed on images of the Silk Road Servers, I have learned the following:

a. Between February 2, 2011 and October 2, 2013, approximately 1.5 million transactions occurred over Silk Road, involving approximately 9.9 million Bitcoin, which generated commissions of approximately 640,000 Bitcoin for Silk Road. PSR ¶ 59. The vast majority of transactions were for illegal narcotics. PSR ¶ 59.

b. Between January 2011 and October 2013, there were approximately 3,748 different registered vendor accounts, and approximately 115,391 registered buyer accounts who

had engaged in at least one transaction on the website. The data indicated a worldwide geographic scope of countries where vendors and buyers indicated that they were located. PSR ¶ 59.

III. Ross Ulbricht's Conviction and Sentencing

11. On February 4, 2015, following a jury trial in the Southern District of New York, defendant Ross Ulbricht, a/k/a "the Dread Pirate Roberts," was convicted on various charges, including charges relating to distributing narcotics by means of the internet and conspiring to commit money laundering, arising out of his role in creating and operating the Silk Road dark-web internet marketplace. On May 29, 2015, Ulbricht was sentenced to life in prison. *See United States v. Ulbricht*, S1 14 Cr. 68.

12. With respect to forfeiture, at Ulbricht's 2015 sentencing, it was undisputed that all 9.9 million Bitcoin that passed through the Silk Road's Bitcoin-based payment system between 2011 and 2013 were directly forfeitable as a result of Ulbricht's crimes, including his money laundering offense. Indeed, it was undisputed at sentencing that, between February 2, 2011 and October 2, 2013, approximately 1.5 million transactions occurred over Silk Road, involving approximately 9.9 million Bitcoin, and these transactions generated commissions of approximately 640,000 Bitcoin for Silk Road. *See* PSR ¶ 59. And at sentencing, the district court concluded that "all funds passing through Silk Road's Bitcoin-based payment system were involved in the money laundering offense in Count Seven. The Bitcoin-based system promoted and facilitated illegal transactions on Silk Road and concealed the proceeds of those transactions. It also concealed the identities of and locations of users." Sentencing Tr. at 92:15-21. Based on evidence that it described as "clear," the district court found, "by far more than a preponderance of the evidence," that Ulbricht was "liable for all the funds that passed through Silk Road regardless of whether he personally retained them." *Id.* at 92:22-93:2. Ulbricht never objected to or substantively challenged this judicial forfeiture determination.

IV. The Investigation Leading to Seizure of the Subsequently Located Silk Road BTC

Summary of Investigation

13. Since 2019, I have been investigating the whereabouts of approximately 53,500 BTC that are directly forfeitable property that were involved in or are traceable to Ulbricht's crimes. Specifically, I have been investigating a September 2012 scheme to defraud Silk Road of at least approximately 50,000 Bitcoin from Silk Road's Bitcoin-based payment system and subsequent efforts to launder this Silk Road BTC. Through the exploitation of a technical vulnerability in Silk Road's infrastructure, an individual ("Individual-1") executed a scheme to defraud Silk Road by unlawfully obtaining at least approximately 50,000 BTC from Silk Road's Bitcoin-based payment system and transferring it into a variety of separate addresses that Individual-1 controlled in an attempt to conceal Individual-1's ownership, obfuscate the source of the funds, and launder these proceeds. In particular, in September 2012, Individual-1 (a) created a string of approximately nine Silk Road accounts (the "Fraud Accounts") in a manner designed to conceal Individual-1's identity; (b) triggered over 140 transactions in rapid succession in order to trick Silk Road's withdrawal-processing system into releasing approximately 50,000 Bitcoin from its Bitcoin-based payment system into Individual-1's accounts; and (c) transferred this Bitcoin into a variety of separate addresses also under Individual-1's control, all in a manner designed to prevent detection, conceal Individual-1's identity and ownership, and obfuscate the Bitcoin's source.

14. Nearly five years after Individual-1's fraud, in August 2017, solely by virtue of Individual-1's possession of the at least approximately 50,000 BTC that Individual-1 unlawfully obtained from Silk Road, Individual-1 received a matching amount of a related cryptocurrency—at least approximately 50,000 Bitcoin Cash ("BCH Crime Proceeds")—on top of the 50,000 BTC

of Silk Road BTC.[1] Individual-1 thereafter exchanged through an overseas cryptocurrency exchange all of the BCH Crime Proceeds for additional Bitcoin, amounting to approximately 3,500 BTC of additional crime proceeds that are traceable to Ulbricht's laundering of criminal proceeds.

15. Collectively, by the last quarter of 2017, Individual-1 thus possessed approximately 53,500 BTC (collectively, the "Silk Road Crime Proceeds") of directly forfeitable crime proceeds.

16. On November 9, 2021, pursuant to a judicially authorized premises search warrant, I, along with my IRS-CI colleagues, seized 50,491.06251844 BTC of the Silk Road Crime Proceeds from one of Individual-1's residences. Using a conservative estimate of the lowest spot price of BTC on the date of the search, the value of the seized BTC at the time of the search was approximately $3.35 billion.[2]

17. On or about March 25, 2022 and May 25, 2022, counsel for Individual-1 voluntarily surrendered to the Government 825.38833159 BTC and 35.4470080 BTC, respectively, of additional BTC that Individual-1 had unlawfully obtained from Silk Road in September 2012. Along with the 50,491.06251844 BTC of BTC that law enforcement seized on November 9, 2021, this results in a total recovery of approximately 51,351.89785803 BTC of the 53,500 Silk Road Crime Proceeds, *i.e.*, the Subsequently Located Silk Road BTC. Using a conservative estimate of the lowest spot price of BTC on the seizure dates, the total value of the Subsequently Located Silk

[1] In August 2017, in a hard fork coin split, Bitcoin split into two cryptocurrencies, traditional Bitcoin and Bitcoin Cash ("BCH"). When this split occurred, any Bitcoin address that had a Bitcoin balance (as Individual-1's did) now had the exact same balance on *both* the Bitcoin blockchain *and* on the Bitcoin Cash blockchain. As of August 2017, Individual-1 thus possessed 50,000 BCH in addition to the 50,000 BTC that Individual-1 unlawfully obtained from Silk Road, solely by virtue of Individual-1's possession of that 50,000 BTC at the time of the August 2017 hard fork.

[2] In addition to this Bitcoin, on November 9, 2021, and thereafter, I seized additional BTC from Individual-1 that is not traceable to the Silk Road. Taking this additional Bitcoin into account, on November 9, 2021 alone, I seized approximately 50,676.17851897 Bitcoin, then valued at over $3.36 billion.

Road BTC is approximately $3.39 billion. All of the Subsequently Located Silk Road BTC was involved in and/or is traceable to defendant Ulbricht's laundering of criminal proceeds. The Subsequently Located Silk Road BTC was seized on the dates specified in the chart below:

Date	**Quantity (BTC)**	**Lowest BTC Spot Price (USD)**	**Total USD Value at Time of Seizure**
November 9, 2021	50,491.06251844	$66,382.06	$3,351,700,741.56
March 25, 2022	825.38833159	$43,706.29	$36,074,661.78
May 25, 2022	35.4470080	$29,384.95	$1,041,608.56
Total:	**51,351.89785803**		**$3,388,817,011.90**

Individual-1 Defrauds Silk Road's Bitcoin-Based Payment System of 50,000 BTC

18. Based on my familiarity with an IRS-CI Cyber Crimes analyst's forensic reviews of images of the Silk Road Servers, I have learned the following:

a. **The Silk Road Servers.** In reviewing images of the Silk Road Servers, an IRS-CI Cyber Crimes analyst analyzed computer databases which contained detailed records for transactions which occurred on Silk Road during the course of its operation. The Silk Road Servers included the following information: accounting ledger of all user activity, deposits, and withdrawals; blockchain information about deposits and withdrawals, including which Silk Road addresses belong to which users; Bitcoin address information; Bitcoin transaction information; vendor/buyer disputes and resolutions; error log; gift codes; internal transfers; private messages between Silk Road users; shipping information; user account information, including account creation information; user feedback; transaction history, including user purchases; user favorites; vendor items for sale; and word filters. And as set forth in Ulbricht's PSR, the Silk Road Servers' transactional database included detailed information regarding each transaction, including the

category of product that was sold, the purchase price, both in Bitcoin and in U.S. dollars, and the commission taken by Silk Road, also in both Bitcoin and U.S. dollars. PSR ¶ 59.

b. As set forth in more detail below, the data described in paragraph 18.a., *supra*, shows that over a period of a few days in September 2012, Individual-1 created a small number of user accounts on the Silk Road dark-web internet marketplace. Individual-1 then used these accounts to exploit a vulnerability in Silk Road's Bitcoin payment processing system and transfer at least approximately 50,000 Bitcoin out from Silk Road's Bitcoin-based payment system, without providing any goods or services in return. That is, Individual-1 created about nine user accounts, and in over 140 transactions occurring in a few days, Individual-1 transferred at least approximately 50,000 Bitcoin from Silk Road's Bitcoin addresses into Individual-1's own addresses, without ever providing any goods or services in return. Individual-1 thereafter moved these Bitcoin out of Silk Road, and, in a matter of days, consolidated them into two high-value amounts—one consisting of approximately 40,000 Bitcoin, and one consisting of approximately 10,000 Bitcoin. At the time of Individual-1's fraud, all of these 50,000 Bitcoin had passed through Silk Road's Bitcoin-based payment system.

c. In particular, beginning on or about September 19, 2012 and continuing over the next few days, Individual-1 created the Fraud Accounts. Some of these accounts, based on the IRS-CI Cyber Crimes analyst's forensic reviews, unlike the majority of the accounts, did not have a basic account profile or an identifiable username, such as Individual-1's newly created account with Silk Road UserID "2c0eed0345." Among the accounts created by Individual-1 with an identifiable username were: "thetormentor," "suxor," "dubba," "gribs," "s1lky," and "imsh." Individual-1 used these accounts to execute the fraud. During this period in September 2012, Individual-1, using the Fraud Accounts, engaged in a scheme or artifice to defraud Silk Road of approximately 50,000 Bitcoin from its Bitcoin-based payment system.

d. While executing the September 2012 fraud, Individual-1 did not list any item or service for sale on the Silk Road, nor did Individual-1 purchase any item or service on Silk Road. In fact, with the sole exception of a single message sent by one of the Fraud Accounts (the content of which is unknown), the Fraud Accounts appear to have been used exclusively to deposit and withdraw Bitcoin from the Silk Road often in rapid succession, as described further below.

e. None of the Fraud Accounts were used or accessed after November 2012.

f. In addition to the unusual pattern of behavior described above, I have learned that for each of the Fraud Accounts associated with an identifiable username, *see supra* ¶ 18(c), Individual-1 registered the accounts by providing the bare minimum of information required by Silk Road to create the account: a username and a password. For instance, although a user registering an account with Silk Road was given the option of providing nationality or country location information, Individual-1 provided no such information for the Fraud Accounts. The Fraud Accounts were merely a conduit for Individual-1 to defraud Silk Road of Bitcoin.

19. Based on my familiarity with an IRS-CI Cyber Crimes analyst's forensic reviews of images of the Silk Road Servers, in conjunction with information contained in the Bitcoin blockchain and records provided by a blockchain tracing provider, I have learned the following about the 50,000 Bitcoin unlawfully obtained by Individual-1:

a. Individual-1 funded the Silk Road addresses associated with the Fraud Accounts with an initial deposit of between 200 and 2,000 Bitcoin per address. After Individual-1 made the initial deposit, Individual-1 then quickly executed a series of withdrawals. Due to a flaw in Silk Road's payment processing system, Individual-1 was able to exploit the withdrawal processing flaw and withdraw many times more Bitcoin out of Silk Road's addresses than Individual-1 had deposited in Individual-1's own addresses in the first instance.

b. By way of example, on or about September 19, 2012, Individual-1, using the Fraud Account associated with username "thetormentor," deposited 500 Bitcoin into one of that account's Silk Road Bitcoin addresses. Less than five seconds after making the initial deposit, "thetormentor" executed five withdrawals of 500 Bitcoin in rapid succession—*i.e.*, within the same second—resulting in a net gain of 2,000 Bitcoin. Within the next 24 minutes, "thetormentor" deposited another 500 Bitcoin into the account's Silk Road Bitcoin address. Within 19 minutes after making that deposit, "thetormentor" again executed three withdrawals of 500 Bitcoin—again, within the same second—which resulted in a net gain of 1,000 Bitcoin. In this manner, "thetormentor" successfully obtained 3,000 Bitcoin in total out of Silk Road on a single day.

c. Similarly, on or about September 20, 2012, Individual-1, using the account "gribs," made an initial deposit of 350 Bitcoin, and a few moments later, executed a series of three withdrawals of 350 Bitcoin each, resulting in a net gain of 700 Bitcoin.

d. Thereafter, Individual-1, using the account with Silk Road UserID "2c0eed0345," made an initial deposit of 2,000 Bitcoin, then executed a series of eight withdrawals of 2,000 Bitcoin each, all of which occurred in rapid succession, resulting in a net gain of 14,000 Bitcoin.

e. As another example, on or about September 24, 2012, Individual-1, using the account "dubba," made approximately one deposit as compared to over 50 Bitcoin withdrawals from Silk Road, resulting in a net gain, before the account ceased its activity.

f. In this fashion, Individual-1, using each of the Fraud Accounts, moved at least approximately 50,000 Bitcoin out of Silk Road in just a few days.[3]

[3] Bitcoin addresses that Individual-1, using the Fraud Accounts, sent Silk Road Crime Proceeds to are: 12hkgmdqps76Bp3e466c2DTGDfg8tKRGLM;
1P1ik9HkCNSs7Zmgc3LzEN72X1Egwm9Chb;
1DwCny29uDhpmd8Mz4hKudwmrSGBdUvrtL;

g. By September 24, 2012, Individual-1 had consolidated the funds outside of Silk Road into two sizeable amounts: a Bitcoin address containing approximately 40,000 Bitcoin, largely funded by the Silk Road exploits of Individual-1's accounts "gribs" and "s1lky," and Individual-1's account with UserID "2c0eed0345"; and a Bitcoin address containing approximately 10,000 Bitcoin, largely funded by the Silk Road exploits of Individual-1's accounts "dubba" and "suxor."[4]

h. For several years after September 24, 2012, Individual-1 maintained the 50,000 Bitcoin that Individual-1 transferred out of the Silk Road in the configuration described immediately above, that is, one address containing approximately 40,000 Bitcoin, and another address containing approximately 10,000 Bitcoin. In the years that have followed the fraud, however, Individual-1 periodically transferred this Bitcoin in bulk to different Bitcoin addresses. In particular, Individual-1 transferred the approximately 40,000 Bitcoin described above to new addresses in or around, among other times, October 2013, March 2015, August 2017, and January

---

13143TYGMgJcGy9KKkL1Y4qnDgTFUF4rMF; 1LDP78Ft3xKwf94jhsxxZjrvA3SGfstQz3; 15cXYu6VWS1qSPf1881pb56CspvNWZDZQf; 1Fqwi5e7wYkdVX5oYE71eJWvTvZYDQ1hsh; 1PjYjjmAYgvcenKAJySCJsS6x8jpVt3XcZ; 1HcEy9PTUHoNy36tsgnJZguacezonPSinL; 162htXpoThKJEY9pSBfeG3fA4Z3DMkiLWY; and 1LoujFHrshc4Zej8nxFPFmMEdan67gvrSa.

From these Bitcoin addresses, Individual-1 transferred some of the Silk Road Crime Proceeds to the following additional Bitcoin addresses: 13GdXePufLt9DipRa5AvG18xLcFNN7TrJY; 1L6QDHZVHnvPnEuF2pzmMPr1N3pz5iH8eU; 16k4aE6mPk7SWqcibBRxLyYp1Q9ozBJ3xg; 1NGzLd3LpDitb5sWihhwrEyhGmnfj3ajUD; and 1N6xxifiiGxonvNAdzZs8M1NNAYNVwPUqq.

[4] Bitcoin addresses controlled by Individual-1 that contained the approximately 40,000 Bitcoin are: 17abSYoj9A7JJU5iqAGcPX74jzL9ELA6Ek; 1GSNd5FcMB3NWbfkvJG2cq5NW1vA7cz3yF; 1DJ8GNR2N8ZFyd5dsNYcA7qF7cqbRksAZZ; and 1BqcwhKevdBKeos72b8E32Swjrp4iDVnjP. The Bitcoin address controlled by Individual-1 containing approximately 10,000 Bitcoin is 18Y8RM9TxunRLmw5MMD4mzY8Q9cYdPivm6.

2018.[5] Likewise, Individual-1 periodically transferred the approximately 10,000 Bitcoin described above in bulk to new addresses in or around, among other times, February 2014, February 2015, August 2017, and November 2017.[6] Then, on May 1, 2019, Individual-1 transferred both the approximately 40,000 Bitcoin and the approximately 10,000 Bitcoin amounts to new addresses.[7]

i. With respect to the 10,000 BTC configuration, in or around November 2020, Individual-1 transferred the 10,000 BTC unlawfully obtained from Silk Road to about 10 Bitcoin addresses containing approximately 1,000 BTC each.[8]

j. Based on information contained in the Bitcoin blockchain, records provided by a blockchain tracing provider, my review of Individual-1's laptop containing detailed ledgers

---

[5] Bitcoin addresses controlled by Individual-1 that Individual-1 transferred the approximately 40,000 Bitcoin to are: 14j6jLececs66ZQ8ew6vTFNiEn2NupacWJ; 19Mz2o9RDABT74SA9njZqMtJXKEzj2qUoH; 1PzGnXGvoGGtCcGpqzkJHebZVgM48VL2x4; 39jzjt85tcRkqki6BeRzsD4FfF6BZKYQnR; and bc1q9sh6544xls87x7skjzyfhkty4wq7z76vn7qzq9.

[6] Bitcoin addresses controlled by Individual-1 that Individual-1 transferred the approximately 10,000 Bitcoin to are: 1AM5xJLHAenvTdzRDh6rv5TUFJm84W4uvT; 1KE2X6GeHPa4NMz22LCabdXHaL6Cva7GC5; 17qwZ8jfXW9K1gcm1RQjiSjGu6vtJt4VzY; 1EBLPT7vEn7Dm7k2JCJC8KNBtrF7n59wY7; 18JY9iVh5zjRh95VTuZKmUEfFNXbu9NhkY; and 3DwBwG6khA63MSCgjrhBRRVpEBibbHuur9.

[7] The Bitcoin addresses controlled by Individual-1 that Individual-1 transferred the approximately 40,000 and 10,000 Bitcoin to on this date, respectively, are bc1q5shngj24323nsrmxv99st02na6srekfctt30ch and bc1q2raxkmk55p000ggfa8euzs9fzq7p4cx4twycx7.

[8] The 10 Bitcoin addresses controlled by Individual-1 containing approximately 1,000 BTC each are: bc1qfj4trvfnute2kkdfxssymq2p6ztj63r68j5d3t; bc1qam27vpg8ve5sd6m7xpz93eexwwm0c4yly9c7u3; bc1q9hv8dx3f5flg3gqc0uprel097yevkvklwzvcvt; bc1qkq4clu886qkgq5rtegesa7jt2lrp7yyujvl96t; bc1qh8srqerlu8m05za0949605fvfttknc9qrp23l4; bc1qwtdggnya06g68vnkyjf7l0lzt7nqz609cq7vt2; bc1qq7rnxtywgqjs0x57gv38y5al0tcanqg0nrj7zx; bc1qc6he83h5v0n6znh95detfnv093jftw3vquzgk8; bc1qnd8zru8xjukvnylv6aj7vjy7ltpzuept93eff2; and bc1q95h6vkehyvnss820w85uz60pnv6qyfuhvtckw8.

spelling out various cryptocurrency transactions, and Individual-1's voluntary surrender to the Government of the Bitcoin described in paragraphs 17 and 28, Individual-1 pushed approximately 750 BTC of the Silk Road Crime Proceeds through a decentralized Bitcoin mixer within the calendar year before the November 9, 2021 search of Individual-1's residence. Based on my training and experience, and public statements and promotional materials made by decentralized Bitcoin mixers, an important and common function served by decentralized Bitcoin mixers is to obfuscate one's control over and the source of Bitcoin.

Other Pre-Search Activity Tying Individual-1 to the Silk Road Crime Proceeds

20. In contemporaneous posts on a Bitcoin message board that I reviewed from 2012, Individual-1 observed that Silk Road stored about 50,000 BTC at a time, the very quantity that Individual-1 unlawfully obtained during the course of Individual-1's fraud scheme.

21. Further, Individual-1 repeatedly boasted, in additional public message board posts that I reviewed, about Individual-1's state-of-the-art computer setup at Individual-1's residences. I have personally observed and can confirm the technical sophistication of Individual-1's home operations. Among other things, at these residences, Individual-1 maintained multiple computer servers, virtual private networks, cold wallets,[9] virtual machines, numerous layers of encryption, and multiple Bitcoin nodes.[10]

[9] The term "cold wallet" refers to the practice of storing Bitcoin offline, often in an encrypted, password-protected storage device known as a hardware wallet. Because Bitcoin is an entirely digital currency, it is vulnerable to theft and misappropriation by hackers if stored online; thus, offline storage in a cold wallet is used to protect the digital currency against online attack.

[10] Based on my training and experience and my conversations with an IRS-CI contractor, I know that a Bitcoin node is a program that validates Bitcoin transactions and stores a copy of all transactions that have ever occurred on the Bitcoin network in its local database.

22. Based on my review of records from an internet service provider, I know that Individual-1 was assigned a unique IP address 45.20.67.1 (the "45 IP Address") for the period from at least August 1, 2016 until at least April 1, 2021.

23. Based on my review of internet service provider records, records from a full-service digital currency prime broker (the "Exchange"), and publicly accessible transaction data on the BTC blockchain, I learned the following information, in substance and in part:

a. Individual-1 opened an account with the Exchange in or around March 2017.

b. Individual-1 periodically accessed Individual-1's account on the Exchange using the 45 IP Address—a unique IP address assigned to Individual-1 by an internet service provider.

c. In 2019, Individual-1 logged onto Individual-1's account on the Exchange from the 45 IP Address and sold approximately 118 BTC to the Exchange. As part of this transaction, change of approximately 0.07750842 BTC was deposited into the following BTC address controlled by Individual-1: bc1qeg2zudacngh7lt6se2vtke7kwdnau9f4p5jv5h (the "Individual-1 v5h Address").

24. As set forth in paragraphs 19.i., 26, and 27, and footnotes 7 and 8, based on my Bitcoin seizures, my review of the detailed ledgers from Individual-1's laptop, my review of the wallet.dat files recovered during the Search from Individual-1's devices storing Silk Road Crime Proceeds, and my review of the Bitcoin blockchain and records provided by a blockchain tracing provider, I know that on or about November 24, 2020, Individual-1 transferred approximately 10,000 of Silk Road Crime Proceeds to approximately 10 BTC addresses that Individual-1 controlled containing approximately 1,000 BTC each. One of these 10 BTC addresses is bc1q95h6vkehyvnss820w85uz60pnv6qyfuhvtckw8. As set forth in paragraph 27, in the detailed

ledgers from Individual-1's laptop, Individual-1 labeled this particular BTC address as "10K-IN." Based on my review of the Bitcoin blockchain and records provided by a blockchain tracing provider, I observed that the 10K-IN BTC address has been on the same input side of cryptocurrency transactions as the Individual-1 v5h Address, indicating that Individual-1 is the common controller and operator of both the Individual-1 v5h Address and the 10K-IN address.[11] That is, the same BTC address controlled by Individual-1 that received change of approximately 0.07750842 BTC in 2019, as indicated in the Exchange records, also is associated with a BTC address that Individual-1 used to transfer 1,000 BTC that Individual-1 had unlawfully obtained from Silk Road. Because Individual-1 later provided law enforcement with access to the Bitcoin that had been stored in the 10K-IN address, I now know that Individual-1, in fact, previously controlled the Silk Road Bitcoin in that address.

V. The November 9, 2021 Search of Individual-1's Residence and the Seizure of the Subsequently Located Silk Road BTC

25. On November 9, 2021, pursuant to a judicially authorized premises search warrant that I executed with IRS-CI colleagues at one of Individual-1's residences (the "Search"), I recovered substantial portions of the Silk Road Crime Proceeds, as well as other valuable assets.

26. Specifically, on November 9, 2021, I seized 50,491.06251844 BTC of the approximately 53,500 Silk Road Crime Proceeds. I located the 50,491.06251844 BTC (a) on devices in an underground floor safe; and (b) on a single-board computer that was submerged under blankets in a popcorn tin stored in a bathroom closet. In addition, I also recovered property

[11] When numerous lesser-value input addresses are used to fund a larger-value transaction, akin in the fiat currency context to using multiple bills and coins to buy a single, higher-value item, this activity is referred to as "common spending" or "co-spending" activity. A collection of cryptocurrency addresses that co-spend (*i.e.*, addresses that are observed to be on the same input side of a transaction) are highly likely to be controlled by the same individual. This process of associating co-spending BTC addresses is known as "grouping" or "clustering."

not traceable to Silk Road, including $661,900 in cash from the underground floor safe and a kitchen drawer, 25 Casascius coins (physical bitcoin) with an approximate value of 174 Bitcoin from the underground floor safe, and metal items from the underground floor safe.[12] Photographs of the underground floor safe and some of its contents are included below:

[12] The metal items consisted of four one-ounce silver-colored bars, three one-ounce gold-colored bars, four 10-ounce silver-colored bars, and one gold-colored coin, all seized from Individual-1's home on November 9, 2021.

As discussed *supra*, using a conservative estimate of the lowest spot price of BTC the date of the Search, the value of the 50,491.06251844 BTC of the Silk Road Crime Proceeds at

the time of the Search was approximately $3.35 billion. Based on my review of the wallet.dat files recovered during the Search from Individual-1's devices then storing substantial portions of the Silk Road Crime Proceeds, conversations with IRS-CI colleagues who also have reviewed the files, and review of the Bitcoin blockchain, the endpoint BTC addresses where the BTC was previously stored were visible in the files, and matched 11 of the applicable BTC addresses in footnotes 5, 6, 7 and 8, *supra*, which trace back to Individual-1's transfers of the Silk Road Crime Proceeds.[13] Additionally, based on my review of the wallet.dat files and conversations with IRS-CI colleagues who also have reviewed the files, the file name labels themselves indicate that 40,000 BTC and 10,000 BTC had been stored on those devices recovered during the Search.

27. During the Search, I also recovered from the living room Individual-1's laptop containing detailed ledgers spelling out cryptocurrency transactions of assets configured in 40,000 and 10,000 blocks—the same configuration as the BTC that Individual-1 had unlawfully obtained from Silk Road in September 2012—involving the Silk Road Crime Proceeds. *See supra* ¶¶ 18, 19, 26. These detailed ledgers show Individual-1's control of the Silk Road Crime Proceeds. For example, as described in footnotes 7 and 8, *supra*, on or around November 24, 2020, Individual-1 sent 1,000 BTC of the 10,000 BTC of Silk Road Crime Proceeds from BTC address bc1q2raxkmk55p000ggfa8euzs9fzq7p4cx4twycx7 to BTC address

[13] Some of the visible addresses in the wallet.dat files recovered during the Search from Individual-1's devices that match 11 of the applicable BTC addresses in footnotes 5, 6, 7 and 8, *supra*, are:
bc1q9sh6544xls87x7skjzyfhkty4wq7z76vn7qzq9;
3DwBwG6khA63MSCgjrhBRRVpEBibbHuur9;
bc1q5shngj24323nsrmxv99st02na6srekfctt30ch;
bc1q2raxkmk55p000ggfa8euzs9fzq7p4cx4twycx7;
bc1qfj4trvfnute2kkdfxssymq2p6ztj63r68j5d3t;
bc1qam27vpg8ve5sd6m7xpz93eexwwm0c4yly9c7u3;
bc1q9hv8dx3f5flg3gqc0uprel097yevkvklwzvcvt; bc1qkq4clu886qkgq5rtegesa7jt2lrp7yyujvl96t;
bc1qwtdggnya06g68vnkyjf7l0lzt7nqz609cq7vt2;
bc1qq7rnxtywgqjs0x57gv38y5al0tcanqg0nrj7zx; and
bc1qc6he83h5v0n6znh95detfnv093jftw3vquzgk8.

bc1q95h6vkehyvnss820w85uz60pnv6qyfuhvtckw8. In the detailed ledgers from Individual-1's laptop, Individual-1 labeled this latter BTC address bc1q95h6vkehyvnss820w85uz60pnv6qyfuhvtckw8 as "10K-IN." Individual-1 similarly labeled numerous transactions involving "BCH40K" and "BCH10K," referring to the BCH Crime Proceeds, showing Individual-1's control of the BCH Crime Proceeds that Individual-1 exchanged for additional Bitcoin. And among other things, the labels and address information contained in the detailed ledgers show that Individual-1 pushed some of the Silk Road Crime Proceeds through a decentralized Bitcoin mixer.

28. Beginning in or around March 2022, counsel for Individual-1 began surrendering to the Government passphrases and instructions for the Silk Road Crime Proceeds then in the Government's possession, as well as for additional Silk Road Crime Proceeds that Individual-1 had access to and had not dissipated. The passphrases and instructions provided by Individual-1 verified Individual-1's prior control of the Silk Road Crime Proceeds. On or about March 25, 2022 and May 25, 2022, counsel for Individual-1 surrendered to the Government an additional 825.38833159 BTC and 35.4470080 BTC (*i.e.*, in addition to what law enforcement seized during the Search), respectively, of the Silk Road Crime Proceeds.

29. All of the Subsequently Located Silk Road BTC is presently located in BTC addresses controlled by the U.S. Government.

30. As discussed *supra*, using a conservative estimate of the lowest spot price of BTC the dates that the BTC was seized, the total value of the Subsequently Located Silk Road BTC is approximately $3.39 billion. The Subsequently Located Silk Road BTC was seized on the dates specified in the chart below:

Date	**Quantity (BTC)**	**Lowest BTC Spot Price (USD)**	**Total USD Value at Time of Seizure**
November 9, 2021	50,491.06251844	$66,382.06	$3,351,700,741.56
March 25, 2022	825.38833159	$43,706.29	$36,074,661.78
May 25, 2022	35.4470080	$29,384.95	$1,041,608.56
Total:	**51,351.89785803**		**$3,388,817,011.90**

31. Based on my review and forensic analysis of the Subsequently Located Silk Road BTC, including my review of the Bitcoin blockchain, records provided by a blockchain tracing provider, Individual-1's laptop ledgers, attribution information contained in the wallet.dat files, the transaction history of the Subsequently Located Silk Road BTC, and Individual-1's sworn plea allocution in 22 Cr. 606 (PGG) (S.D.N.Y.) that occurred on November 4, 2022, all of the Subsequently Located Silk Road BTC was involved in or is traceable to Ulbricht's laundering of criminal proceeds. With respect to the approximately 50,000 BTC that Individual-1 unlawfully obtained in 2012, at the time of Individual-1's fraud, all of these 50,000 Bitcoin had passed through Silk Road's Bitcoin-based payment system; indeed, Individual-1 unlawfully obtained them directly from Silk Road's Bitcoin-based payment system. These 50,000 Bitcoin are the same Bitcoin that Individual-1 then periodically transferred in bulk to different addresses in the following years until they were recovered by law enforcement, as described above. As for the 3,500 BTC that Individual-1 obtained in 2017, Individual-1 obtained the BCH Crime Proceeds solely by virtue of Individual-1's possession of 50,000 of the Silk Road Crime Proceeds at the time of the August 2017 hard fork. These BCH Crime Proceeds are thus also property traceable to the forfeitable 9.9 million Silk Road Bitcoin that passed through Silk Road's Bitcoin-based payment system between 2011 and 2013. By exchanging through an overseas cryptocurrency exchange all

of the BCH Crime Proceeds for additional Bitcoin, Individual-1 obtained approximately 3,500 BTC of additional crime proceeds that are traceable to Ulbricht's money laundering count of conviction.

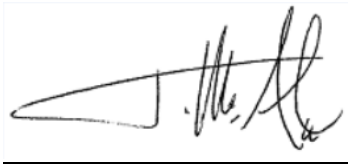
32. Based on my review of the plea agreement, I have learned that on or about October 26, 2022, Individual-1 signed a plea agreement with the Government wherein Individual-1 agreed to plead guilty in a standalone criminal case, 22 Cr. 606 (PGG) (S.D.N.Y.), to wire fraud, in violation of 18 U.S.C. § 1343, for Individual-1's 2012 scheme to defraud Silk Road of Bitcoin (the "Individual-1 Plea Agreement"). In the Individual-1 Plea Agreement, Individual-1 also agreed to forfeit, among other things, all Bitcoin traceable to the offense and various additional assets.

33. Based on my observation of Individual-1's November 4, 2022 change of plea hearing in 22 Cr. 606 (PGG) (S.D.N.Y.), I know that on that date Individual-1 pleaded guilty to wire fraud, in violation of 18 U.S.C. § 1343, pursuant to the Individual-1 Plea Agreement. During Individual-1's sworn plea allocution, Individual-1 admitted, in sum and substance, to have executed a scheme to defraud Silk Road of approximately 50,000 Bitcoin in September 2012. In sum and substance, Individual-1 admitted, over a number of days in September 2012, to have engaged in a scheme to defraud Silk Road of money and property, specifically, approximately 50,000 Bitcoin, by (a) creating a string of Silk Road accounts in a manner designed to conceal Individual-1's identity; (b) triggering multiple transactions in rapid succession in order to trick Silk Road into releasing Bitcoin from Silk Road's Bitcoin-based payment system into these accounts; and (c) transferring this Bitcoin into a variety of separate addresses also under Individual-1's control, all in a manner designed to prevent detection and conceal Individual-1's identity.

* * *

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

Dated: New York, New York
November 7, 2022



TREVOR McALEENAN
Special Agent
IRS-CI