Approved: _____ 14 MAG 0164
SERRIN TURNER
Assistant United States Attorney

Before: HONORABLE MICHAEL H. DOLINGER
United States Magistrate Judge
Southern District of New York

| | |
|---|---|
| UNITED STATES OF AMERICA<br><br>- v. -<br><br>ROBERT M. FAIELLA,<br>a/k/a "BTCKing," and<br>CHARLIE SHREM,<br><br>Defendants. | SEALED COMPLAINT<br><br>Violations of<br>18 U.S.C. §§ 1960 & 1956;<br>31 U.S.C. §§ 5318(g) &<br>5322(a)<br><br>COUNTY OF OFFENSE:<br>NEW YORK |

SOUTHERN DISTRICT OF NEW YORK, ss.:

Gary L. Alford, being duly sworn, deposes and says that he is a Special Agent with Internal Revenue Service-Criminal Investigation, assigned to the New York Organized Crime Drug Enforcement Strike Force, and charges as follows:

COUNT ONE
(Operating an Unlicensed Money Transmitting Business)

1. From in or about December 2011, up to and including in or about October 2013, in the Southern District of New York and elsewhere, ROBERT M. FAIELLA, a/k/a "BTCKing," the defendant, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of a money transmitting business affecting interstate and foreign commerce, to wit, a Bitcoin exchange service FAIELLA operated on the "Silk Road" website under the username "BTCKing," which (i) failed to comply with the money transmitting business registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations prescribed thereunder, and (ii) otherwise involved the transportation and transmission of funds known to FAIELLA to have been intended to be used to promote and support unlawful activity, to wit, narcotics trafficking on the "Silk Road" website, in violation of Title 21, United States Code, Sections 812, 841, and 846.

(Title 18, United States Code, Section 1960.)

COUNT TWO
(Operating an Unlicensed Money Transmitting Business)

2. From in or about December 2011, up to and including in or about October 2012, in the Southern District of New York and elsewhere, CHARLIE SHREM, the defendant, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of a money transmitting business affecting interstate and foreign commerce, to wit, a Bitcoin exchange service as to which SHREM was the Chief Executive Officer, which involved the transportation and transmission of funds known to SHREM to have been intended to be used to promote and support unlawful activity, to wit, the operation of an unlicensed money transmitting business on "Silk Road" in violation of Title 18, United States Code, Section 1960, and, ultimately, narcotics trafficking on the "Silk Road" website, in violation of Title 21, United States Code, Sections 812, 841, and 846.

(Title 18, United States Code, Section 1960.)

COUNT THREE
(Money Laundering Conspiracy)

3. From in or about December 2011, up to and including in or about October 2012, in the Southern District of New York and elsewhere, ROBERT M. FAIELLA, a/k/a "BTCKing," and CHARLIE SHREM, the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit money laundering.

4. It was a part and an object of the conspiracy that ROBERT M. FAIELLA, a/k/a "BTCKing," and CHARLIE SHREM, the defendants, and others known and unknown, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds from places in the United States to and through places outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, operating an unlicensed money transmitting business and narcotics trafficking, in violation of Title 18, United States Code, Section 1960, and Title 21, United States Code, Section 812, 841, and 846, respectively, all in violation of Title 18, United States Code, Section 1956(a)(2)(A).

Overt Acts

5. In furtherance of said conspiracy and to effect the illegal object thereof, the following overt acts, among others,

were committed in the Southern District of New York and elsewhere:

a. On or about January 17, 2012, ROBERT M. FAIELLA, a/k/a "BTCKing," the defendant, while operating a Bitcoin exchange service on the "Silk Road" website, received multiple orders for Bitcoins from users of the site.

b. On or about January 17, 2012, CHARLIE SHREM, the defendant, filled the orders by causing funds to be transferred to an account that FAIELLA controlled at a third-party Bitcoin exchange service based in Japan.

(Title 18, United States Code, Section 1956(h).)

COUNT FOUR
(Willful Failure to File Suspicious Activity Report)

6. From in or about December 2011, up to and including in or about October 2012, in the Southern District of New York and elsewhere, CHARLIE SHREM, the defendant, willfully failed to report suspicious transactions relevant to possible violations of laws and regulations, as required by the Secretary of Treasury, to wit, SHREM failed to file any Suspicious Activity Report with respect to numerous Bitcoin purchases conducted by ROBERT M. FAIELLA, a/k/a "BTCKing," through a Bitcoin exchange service operated by SHREM.

(Title 31, United States Code, Sections 5318(g) and 5322(a); and Title 31, Code of Federal Regulations, Section 1022.320)

* * *

The bases for my knowledge and for the foregoing charges are as follows:

7. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts learned through my investigation. 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.

## OVERVIEW

8. From in or about December 2011 up to and including in or about October 2013, ROBERT M. FAIELLA, a/k/a "BTCKing," the defendant, ran an underground Bitcoin exchange on an illegal website known as "Silk Road," an anonymous marketplace for illicit drugs. Operating under the username "BTCKing," FAIELLA sold Bitcoins - the only form of payment accepted on Silk Road - to users seeking to make drug buys on the site.

9. Upon receiving orders for Bitcoins from Silk Road users, FAIELLA filled the orders through a company based in New York, New York (the "Company"). The Company enabled customers to exchange cash for Bitcoins anonymously, that is, without providing any personal identifying information, charging a fee for its service. FAIELLA obtained Bitcoins with the Company's assistance, and then sold the Bitcoins to Silk Road users at a markup.

10. From in or about August 2011 until in or about July 2013, when the Company ceased operating, CHARLIE SHREM, the defendant, was the Chief Executive Officer of the Company. SHREM was also the Company's Compliance Officer, in charge of ensuring its compliance with anti-money laundering ("AML") laws. Beyond these roles at the Company, SHREM was and is the Vice Chairman of a foundation dedicated to promoting the Bitcoin virtual currency system.

11. As set forth below, notwithstanding that SHREM was aware that Silk Road was a drug-trafficking website, and that FAIELLA was running a Bitcoin exchange service there, SHREM knowingly helped FAIELLA conduct his operation through the Company in light of the substantial income the Company received from his business. Not only did SHREM knowingly allow FAIELLA to use the Company's services to buy Bitcoins for his Silk Road customers, he personally processed FAIELLA's transactions, gave FAIELLA discounts on his high-volume orders, willfully failed to file suspicious activity reports about FAIELLA, and deliberately helped FAIELLA circumvent the Company's AML restrictions, even though it was SHREM's job to enforce them. Working together, SHREM and FAIELLA exchanged over $1 million in cash for Bitcoins for the benefit of Silk Road users, so that they could, in turn, make illicit purchases on Silk Road.

12. SHREM and FAIELLA eventually parted ways after the Company stopped accepting cash payments for Bitcoins in late 2012. FAIELLA temporarily shut down his illegal Bitcoin exchange service on Silk Road as a result. However, FAIELLA

resumed operating on Silk Road in April 2013, without the Company's assistance, and continued to exchange tens of thousands of dollars a week until the Silk Road website was shut down by law enforcement in October 2013.

## BACKGROUND

### The Silk Road Website and Its Bitcoin-Based Payment System

13. The Silk Road website was established in January 2011 and operated until October 2, 2013, when it was seized by law enforcement. Through undercover activity on the site by myself and other law enforcement agents, I learned the following:

a. The Silk Road website hosted an online black-market bazaar, allowing vendors and buyers to conduct illicit transactions over the Internet.

b. Silk Road was only accessible through the Tor network, a special network on the Internet designed to conceal the true IP addresses of the computers on the network, and, thereby, the identities of the network's users.

c. The illegal nature of the commerce hosted on Silk Road was readily apparent to anyone visiting the site. The vast majority of the goods for sale consisted of illegal drugs of nearly every variety, openly advertised on the site as such and prominently visible on the home page.

d. The only form of payment accepted on Silk Road was Bitcoins.

14. Based on my experience in this investigation, I know the following about Bitcoins:

a. Bitcoins are a form of virtual currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a decentralized, "peer-to-peer" network.

b. To acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of conventional currency, which they exchange for a corresponding number of Bitcoins based on a fluctuating exchange rate.

c. When a user acquires Bitcoins, the Bitcoins are sent to the user's Bitcoin "address," analogous to a bank account number, which is designated by a complex string of letters and numbers. The user can then conduct transactions with other Bitcoin users, by transferring Bitcoins to their Bitcoin addresses, via the Internet.

d. No identifying information about the payor or payee is transmitted in a Bitcoin transaction. Only the Bitcoin addresses of the parties are needed for the transaction, which by themselves do not reflect any identifying information.

e. Bitcoins are not inherently illegal and have known legitimate uses, but they are also known to be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move money anonymously.

f. Every Silk Road user had a Bitcoin address associated with the user's Silk Road account. To make purchases on the site, the user first had to obtain Bitcoins (e.g., from an exchanger) and have them sent to the user's Silk Road Bitcoin address. After thus funding his account, the user could make purchases from Silk Road vendors.

Regulation of Bitcoin Exchangers

15. Based on my training and experience, I know the following about regulation of Bitcoin exchangers:

a. Exchangers of virtual currency, including Bitcoin exchangers, are considered money transmitters under federal law and are subject to federal AML regulations if they do substantial business in the United States. See 31 C.F.R. § 1010.100(ff)(5); see also Department of the Treasury Financial Crimes Enforcement Network, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013, FIN-2013-G001, available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

b. Specifically, federal regulations require a virtual currency exchanger to register with the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") as a money services business and to develop and maintain an effective AML program. See 31 C.F.R. §§ 1022.210, 1022.380.

c. Maintaining an effective AML program requires filing Suspicious Activity Reports with FinCEN when appropriate, including reporting substantial transactions or patterns of transactions involving the use of the money services business to facilitate criminal activity. See 31 C.F.R. § 1022.320.

d. Maintaining an effective AML program also requires implementing effective means of verifying customer identities. See 31 C.F.R. § 1022.210(d)(i)(A). In particular, money services businesses must, at a minimum, verify and keep a record of the identity of any customer involved in a transmission of funds of $3,000 or more. See 31 C.F.R. §§ 1010.410, 1022.400.

## Background on the Company

16. The Company is a New York corporation with its principal place of business in New York, New York.

17. From visiting the Company's website[1], I have learned the following:

a. The Company was founded by CHARLIE SHREM, the defendant, and another individual not named herein (the "Co-Founder"). The website listed SHREM as the CEO of the Company and the Co-Founder as the Chief Technology Officer.

b. The Company's website enabled customers to purchase Bitcoins in exchange for cash, although the Company did not sell Bitcoins to customers directly. Instead, the Company transferred funds to its customers at accounts they had at certain third-party Bitcoin exchange services, where they could then convert the funds into Bitcoins. The website explained:

> You pay us an amount equal to whatever you wish to be deposited into your exchange account plus a small commission and at the same time we make a direct transfer at the exchange side from our account to yours.

c. The Company claimed that its system enabled customers to transfer funds into their exchange accounts faster than the methods used by the third-party exchangers themselves, such as wire transfers.

---

[1] The website operated from in or about August 2011 until in or about July 2013, when an announcement was posted that the Company had decided to temporarily "close shop" to redesign its services. The website has not resumed operation since.

d. Moreover, the Company's system enabled customers to move money to their exchange accounts anonymously, since, in order to place an order on the Company's website, users were generally not required to provide any identifying information other than an e-mail address.

e. Customers paid cash to the Company by depositing it in person into a bank account of a certain third-party service the Company used to process these payments (the "Cash Processor").

18. Based on undercover transactions conducted in this investigation, and reviews of e-mail accounts maintained by the Company and the Cash Processor, I know that a typical Bitcoin purchase made through the Company worked as follows:

a. The customer placed an order on the Company's website for a certain dollar amount's worth of Bitcoins, specifying the account number at the third-party Bitcoin exchange where he wanted to obtain the Bitcoins. The customer also provided an e-mail address where he could be contacted about the order.

b. At the Company's direction, the Cash Processor would then e-mail the customer an invoice with instructions on how to deposit the cash payment for the order. The invoice would specify an exact amount of cash needed for the deposit, which would include both the value of the customer's order as well as a nominal "handling fee," used merely to keep track of the transaction. For example, for an order of $200 worth of Bitcoins, the invoice might instruct the customer to deposit $200.32, with the extra 32 cents used by the Company and the Cash Processor to match the deposit, when it came through, to the otherwise anonymous customer. (Thus, no two transactions on a given day would be assessed the same "handling fee.")

c. The invoice would also specify a particular bank, and a bank account there controlled by the Cash Processor, where the cash would need to be deposited. The customer would make the deposit in person by visiting a local branch of the bank.

d. Once the deposit was confirmed by the bank, the Cash Processor would notify the Company, at which point the Company would transfer funds from its account at the third-party Bitcoin exchange selected by the customer, to the customer's own account at the exchange. The Company's commission (ranging from 2 to 10 percent) would be subtracted from the transfer.

e. The customer could then visit the website of the selected third-party exchange, log into his account there, and convert the funds received from the Company into Bitcoins.

The Company's Stated Anti-Money Laundering Policies

19. From reviewing information obtained from FinCEN, I have learned that, on March 26, 2012, the Company registered with FinCEN as a money services business. As set forth above, money services businesses are obligated under federal law to develop and implement an effective AML program.

20. From the Company's website, I have learned that, as part of its AML program, the Company limited cash deposits to under $1,000 per customer per day. The website explained:

> [W]e are simply not allowed by law to handle extremely large amounts of money for a single user without conducting a lot of background checks and having paperwork on file. VERY large transactions would even require us to file notices for the use of law enforcement in tracking money laundering or other criminal activity. . . .
>
> Q: But I want to launder a huge pile of funds! Why are you turning me away?
>
> Because we will not have criminals as clients and will not assist money laundering operations. Please see our AML (Anti Money Laundering) policy for more information.

21. The Company's AML policy, which was set forth on its website, further explained:

a. "[T]he Company opposes money laundering, financing terrorism, and all other illegal uses of the Bitcoin network."

b. SHREM was the Company's "AML Program Compliance Officer," with "full responsibility for the Company's AML Program," because he had "the most comprehensive understanding of the customer flow through the Company's system" and "access to all parts of the approval process" for customer transactions.

c. As Compliance Officer, SHREM was responsible for monitoring transactions for "red flags" and "report[ing] suspicious activities to the appropriate authorities." Examples of "red flags" that SHREM was to look for included any reason to believe a customer was intending to "move illicit cash out of the government's reach," "engage in money laundering," or

"otherwise engage in illegal activity." Other red flags included attempts by a customer to "conduct frequent or large transactions" or to obtain "exemptions from [the Company's] AML Program or other relevant policies."

d. Customers were required to verify their identities before placing any order or "series of orders" of $3,000 or more. Further, "[i]f the Company ha[d] knowledge that the person placing such a payment order [was] not the paying party himself" - that is, if the Company knew someone was placing a $3,000 order or series of orders on behalf of someone else - then the Company would "obtain and retain a record of the paying party's taxpayer identification number."[2]

## THE SILK ROAD BITCOIN EXCHANGER KNOWN AS "BTCKING"

22. From undercover law enforcement activity on Silk Road, I have learned that, in or about December 2011, a Silk Road user known as "BTCKing" began operating a Bitcoin exchange service on the site, selling Bitcoins to Silk Road users in exchange for cash. "BTCKing" advertised his service directly on Silk Road, as in the following posting from March 2012:

> ***FOR THE FASTEST SERVICE place an order by getting one of our "listings" below, include AMOUNT of Bitcoin you want . . . . Don't go far, our response is Very Fast!! . . . .
>
> -We will reply with our bank name and account number for you to make a "cash deposit." . . . Your name is NOT needed and no slips to fill out if you don't want… You could even go to the Drive-Thru!!
>
> -Send us a message that you have made the deposit and you will receive your Bitcoin at the best possible price . . . to your SR account INSTANTLY… Most times the Bitcoin is in your SR account by the time you get back from the bank.
>
> THAT'S IT,…EASY…CHEAP…FAST…[3]

---

[2] As indicated in paragraph 20, the Company limited cash deposits to $1,000 per day to avoid ever triggering such requirements.

[3] Unless otherwise noted, quotations from electronic communications contained herein are reproduced as they appear in the original. Errors in spelling and punctuation have not been corrected. Ellipses appearing in the original are reflected as

23. On August 15, 2012, an undercover agent posing as a Silk Road user ("UC-1") executed a purchase of Bitcoins from "BTCKing," as follows:

a. Through Silk Road's private message system,[4] UC-1 placed an order with "BTCKing" for $500 worth of Bitcoins.

b. "BTCKing" replied with instructions to UC-1 to "deposit EXACTLY $500.11 CASH" into a specific account at a particular bank.

c. Later that day, UC-1 traveled to the designated bank and deposited $500.11 cash into the designated account.

d. Later that same day, UC-1 logged into UC-1's account on Silk Road and observed that approximately $444 worth of Bitcoins had been sent to UC-1's Silk Road Bitcoin address. UC-1 also saw that "BTCKing" had sent UC-1 a message stating that he had charged a $56 fee for the transaction.

24. On October 10, 2012, UC-1 executed a second purchase from "BTCKing" in a similar manner. On this occasion, "BTCKing" instructed UC-1 to deposit exactly $507.10 into a different bank account, which UC-1 did. Later that day, approximately $444 in Bitcoins was sent to UC-1's Silk Road Bitcoin address, and UC-1 received a message from "BTCKing" explaining that the rest of UC-1's deposit had been applied toward "BTCKing's" commission.

25. I have reviewed bank records for the two accounts where "BTCKing" instructed UC-1 to make the deposits involved in these undercover transactions. The records reveal that the accounts were controlled by the Cash Processor that the Company used to receive its cash deposits.

26. On or about February 27, 2013, the Government obtained a search warrant for an e-mail account used by the Cash Processor (the "Cash Processor E-mail Account"). From reviewing the account, I was able to identify invoices corresponding to the deposits UC-1 made in the undercover transactions. The first invoice was sent to the e-mail address "56btc@safe-mail.net," while the second was sent to "12btc@safe-mail.net." UC-1 did not supply any e-mail address as part of the undercover

---

dots without spaces ("…"), while ellipses reflecting omissions from the original are reflected as dots with spaces (". . .").

[4] Silk Road had a private-messaging system that enabled users to send private messages to one another (akin to e-mails).

transactions, nor did UC-1 interact with the Cash Processor in any way. Accordingly, I believe the two e-mail addresses belonged to "BTCKing."

27. I have found approximately 350 invoices in the Cash Processor E-mail Account associated with the "56btc@safe-mail.net" address, and approximately 124 invoices associated with the "12btc@safe-mail.net" e-mail address. In total, I have found approximately 3,000 invoices in the Cash Processor E-mail Account associated with various "safe-mail.net" addresses, many of which have "btc" in the username (including "BTCKing@safe-mail.net"). I have also found various e-mails sent from these e-mail accounts to the Cash Processor E-mail Account, which are often signed the same way, simply with the initial "B" - suggesting that the same user operated all of the accounts.

28. Based on these invoices, and other evidence detailed further below, I believe that "BTCKing" used the Company to obtain his supply of Bitcoins. Specifically:

a. For every Bitcoin order that "BTCKing" received from a Silk Road customer, "BTCKing" would submit a corresponding order for Bitcoins through the Company's website.

b. "BTCKing" would provide his own account at a particular third-party exchange service (the "Third Party Exchange") as the destination for each order, and would provide one of his "safe-mail.net" accounts as the e-mail address where the Company could contact him about the order.

c. Once each order was placed, the Cash Processor would send "BTCKing" an invoice with deposit instructions. "BTCKing" would pass along these instructions to his Silk Road customer through Silk Road's messaging system.

d. Once the customer made the cash deposit, the Company would transfer an equivalent amount of funds (minus the Company's fee) to "BTCKing's" account at the Third Party Exchange, where "BTCKing" would redeem the funds for Bitcoins.

e. Finally, "BTCKing" would send the Bitcoins (minus his own fee) to his customer's Bitcoin address on Silk Road, for the customer to use in making buys from Silk Road vendors.

## "BTCKING'S" PARTNERSHIP IN 2012 WITH CHARLIE SHREM

29. I have reviewed the contents of certain e-mail accounts belonging to SHREM, obtained pursuant to a search warrant (the "Shrem E-mail Accounts"). As described below, the

Shrem E-mail Accounts reflect that "BTCKing" not only obtained his supply of Bitcoins through the Company, but did so with extensive support from SHREM. Even though SHREM quickly realized that "BTCKing" was reselling Bitcoins on Silk Road, which SHREM knew to be a marketplace for illicit drugs, SHREM went out of his way to facilitate "BTCKing's" business. Among other things, SHREM: permitted "BTCKing" to continue doing business with the Company, despite initially threatening to "ban" him based on his illegal activity; personally ensured that "BTCKing's" orders with the Company were filled everyday; gave "BTCKing" discounts based on his large order volume; sought to conceal "BTCKing's" activity from the Co-Founder and the Cash Processor to prevent "BTCKing's" orders from being blocked; advised "BTCKing" how to evade the transaction limits imposed by the Company's own AML policy; let "BTCKing" conduct large transactions without ever verifying his identity, in violation of federal AML laws; and failed to file a single Suspicious Activity Report about "BTCKing," despite the obvious "red flags" raised by "BTCKing's" dealings with the Company.

## SHREM's Knowledge and Facilitation of "BTCKing's" Illegal Business

30. "BTCKing" first came to SHREM's attention in December 2011. Specifically, on December 28, 2011, SHREM e-mailed "BTCKing@safe-mail.net" about two deposits the Company had received, tied to orders placed with that e-mail address. SHREM asked why "you" had made one of the deposits by check instead of cash (as the Company required) and had deposited the wrong amount for the other. "BTCKing" replied that "our customer thought it would be OK" to use a check for the first deposit, and apologized for the wrong amount of the other deposit, explaining, "we are a new company still working out the Kinks." Based on my experience in this investigation, I believe that, before this exchange, SHREM was unfamiliar with "BTCKing's" business and did not yet know that "BTCKing" was placing orders on behalf of others.

31. Within a few days, however, SHREM realized that "BTCKing" was buying Bitcoins through the Company and reselling them. On January 1, 2012, "BTCKing" (using the address "1btck@safe-mail.net") wrote to SHREM, stating he was having problems receiving "invoices" from the Cash Processor after placing orders on the Company's website. SHREM forwarded the message to the CEO of the Cash Processor (the "Cash Processor CEO"). The Cash Processor CEO replied that this user was "creating multiple invoices daily" and asked SHREM to "explain

his activity." SHREM responded, "I think he's some sort of reseller."

32. By January 17, 2012, SHREM knew that "BTCKing" was reselling Bitcoins on Silk Road. In a lengthy exchange of e-mails on that date, after telling "BTCKing" that he knew "BTCKing" was operating on Silk Road, SHREM first purported to ban "BTCKing" from doing business with the Company, copying the Cash Processor and SHREM's business partner, the Co-Founder, on that message. However, SHREM thereafter wrote to "BTCKing" privately, with a different message, advising him how to continue using the Company's services surreptitiously. The exchange went as follows:

a. SHREM sent "BTCKing" the following e-mail, copying the Cash Processor CEO and the Co-Founder:

> We just received notice that you deposited $4,000 today at a bank for a [Company] transfer.
>
> We have warned you in the past you CANNOT deposit more than $1,000 per person per day according to our limits. You have violated our Terms of Service and we know you are reselling your services on The Silk Road. This is illegal. [emphasis in original]
>
> You are hereby banned from our services . . . .
>
> We have all of your deposits on record, your picture from bank security cameras, and branch locations. Any attempt at a new transfer will result in criminal prosecution. [emphasis in original]

b. "BTCKing" replied that his impression was that the Company's deposit limit was $4,000 rather than $1,000. "BTCKing" added: "Are you taking this money, if so I am calling the federal Government as I have broken no laws and you are illegally taking my money...I am just reselling BTC, please reply!!!"

c. SHREM replied, again copying the Cash Processor CEO and the Co-Founder, telling "BTCKing" he was wrong about the Company's deposit limit, and further stating, "Do not threaten me, as you currently sell your services on the illegal Silk Road. We are a licensed MSB [money services business] so your information is already being given to the Federal Financial Crimes Enforcement Network." In fact, I have checked FinCEN records and the Company did not submit any report to FinCEN at this time, or at any other time.

d. "BTCKing" responded, "I am not afraid of the law as I am just selling BTC, just like you. . . . Don't take this poor guys money as it is not mine, he is unknowing of your limits and just buying BTC."

e. SHREM replied, again copying the Cash Processor CEO and the Co-Founder: "We're not taking anyone's money, it will be released within 24 hours - those are the legal rules."

f. At this point in the exchange, the Co-Founder e-mailed "BTCKing" as well, copying SHREM and the Cash Processor CEO: "To clarify: As you have broken our TOS [terms of service] and acted in an illegal manner, we are unwilling to do further business with you. . . . [A]ny attempts to make further deposits using deception will be treated as criminal activity."

g. SHREM followed up, again copying the Co-Founder and the Cash Processor CEO, telling "BTCKing" that his three pending cash deposits would be cleared, but that "[i]n the future, your email address is banned."

h. "BTCKing" wrote back to SHREM, thanking him for releasing the pending deposits, and adding, "I do not wish to cause you problems and can respect your wishes."

i. SHREM replied, but this time he wrote "BTCKing" privately, without copying the Co-Founder or the Cash Processor CEO; and his message considerably changed. SHREM stated: "No problem, in the future please have your customers respect our $1,000 limit. Your e-mail address is banned, but you can use a different one." Based on my experience in this investigation, I believe SHREM meant that the Company would be placing a block on the e-mail address "BTCKing" had used for the problematic transactions, so that "BTCKing" could no longer use this same e-mail address to place orders on the Company's website, but that "BTCKing" could circumvent this restriction by simply using a different e-mail address for future orders.

33. "BTCKing" followed SHREM's advice and continued doing business with the Company using different e-mail addresses. For example, on January 25, 2012, "BTCKing" (now using the address "12btc@safe-mail.net") sent a customer support inquiry to the Company, which was routed to an e-mail account monitored by SHREM and the Co-Founder. SHREM, copying the Co-Founder, replied, "OK, we will look into it." The following exchange then occurred between SHREM and the Co-Founder:

Co-Founder: DO NOT reply to all - doesn't this guy seem a little too similar to the one we banned a while back? I suspect the deposit was not by him but by one of his silk road clients.

SHREM: It probably is, but as long as the person depositing has done less then $1,000 were in the clear

Co-Founder: Shouldn't we stick to bans we impose rather than just letting it slip after threatening criminal prosecution? Makes us look a bit stupid to say the least.

SHREM: We never imposed a ban. I threatened a ban to himself depositing more than $1000. I told him that he has to respect the[] Limits and he is not allowed to personally deposits anymore

Co-Founder: The guy still strikes me as pretty deceptive in using alt e-mail addresses etc - we need to keep a very tight watch on this one

SHREM: You got it boss

34. On January 28, 2012, "BTCKing" (this time using the address "34btc@safe-mail.net") sent another customer support inquiry to the Company, prompting the following exchange:

a. SHREM wrote to "BTCKing" as follows, copying the Co-Founder and the Cash Processor CEO:

> You are causing us alot of issues. I have asked you many time, make sure your customers deposit the EXACT amount. Now your causing us to look into these issues on a weekend.
>
> If your customers don't deposit the EXACT amount next time we will NOT credit you on the exchange and this time ban you for good, not just your e-mail address.

b. The Co-Founder then wrote separately to SHREM: "Let's just ban the guy already."

c. SHREM replied: "Let's focus on resolving this issue the[n] worry about banning him[.] He brings us a lot of business and we won't be able to ban him anyways, he can change all his details."

d. The Co-Founder responded: "You said you found him on silk road, he's obviously trying to be a meta layer over us and selling BTC there and possibly even not telling his customers that it's our service moving the funds. Advertise us on silk road, and then ban him. . . . This way we still get the same level of business . . . , possibly even increasing it and get less fuss."

e. SHREM replied that banning someone because he is an "inconvenience" is "bad business," adding: "He has not broken a law and silk road itself is not illegal. We also don't have any rules against resellers. We make good profit from him."

f. The Co-Founder responded: "It's not because I don't like him or he's an inconvenience . . . , it's because so many of his transactions smell like fraud or money laundering."

g. SHREM replied, simply, "Cool."

35. Notwithstanding SHREM's remark to the Co-Founder that "silk road itself is not illegal," other evidence reflects that SHREM well understood Silk Road's illegal nature. Indeed, as described in paragraph 32 above, just days earlier SHREM had told "BTCKing" that the Company knew he was operating on the "illegal Silk Road" website and threatened to report "BTCKing" to law enforcement on that basis. Moreover, SHREM's e-mails with others reflect that he was personally familiar with Silk Road and understood it was a drug-trafficking website. For example:

a. SHREM's e-mails contain a record of an online chat with an individual not named herein on or about February 1, 2012, in which SHREM wrote, "wow, Silk Road actually works," explaining that he had just received a shipment of marijuana "Brownies."

b. On April 1, 2012, another individual not named herein sent SHREM an e-mail, stating: "You often praise Bitcoin quite easily but my friend was telling me . . . about the Dark Web being used by drug dealers in the UK." SHREM replied: "Yes, its true. Silk Road which can only be viewed through Tor sells any type of drug available. It funds a decent percentage of the overall Bitcoin economy."

36. Other e-mails show that SHREM likewise understood that "BTCKing's" Bitcoin exchange business on Silk Road was illegal

and that "BTCKing" was seeking to evade detection by law enforcement. For example:

a. On February 22, 2012, after SHREM had resolved a problem with one of "BTCKing's" orders, the following exchange occurred between them:

i. SHREM told "BTCKing," "I just want to let you know, I take care of you bro."

ii. "BTCKing" replied, "I'm probably old enough to be your father," to which SHREM quipped in response, "The art of hiding, is making people think you are someone else." Based on the investigation, I believe that SHREM was referring to the fact that "BTCKing" was operating anonymously in doing business with the Company and that, as a result, SHREM did not know "BTCKing's" true identity, including his age.

iii. "BTCKing" replied, "You must understand that the people that we pay taxes to have a long reach and I like to stay away from that." Based on my experience in the investigation, I believe "BTCKing" meant that he was operating anonymously to avoid apprehension by law enforcement.

b. On July 30 and 31, 2013, SHREM received several e-mails from the Cash Processor CEO noting $13,000 in transactions in a single day by someone using the e-mail address "111a@safe-mail.net," and asking SHREM what he knew about the user. Rather than tell the Cash Processor CEO the truth - that the address belonged to "BTCKing," who was reselling Bitcoins on Silk Road - SHREM instead promptly took steps to keep the Cash Processor CEO from discovering "BTCKing's" illegal activity:

i. On August 1, 2013, SHREM wrote to "BTCKing" to warn him that his "111a email address was flagged by [the Cash Processor]" and that he needed to "stop using" it.

ii. "BTCKing" asked SHREM why the account had been flagged.

iii. SHREM responded: "[The Cash Processor] is the one who is making a big deal over this. They don't like that you do so many transactions since they have no idea where you sell, and I cant tell them SR [Silk Road]. You should use a few different emails if you can, that's what they m[o]n[i]tor."

37. SHREM not only knowingly permitted "BTCKing" to operate his illegal business using the Company's services, he

also affirmatively facilitated "BTCKing's" business, by, among other things, working closely with "BTCKing" to make sure "BTCKing's" orders were effectively processed everyday. E-mail communications reflect SHREM personally intervening on a regular basis to resolve glitches with "BTCKing's" orders. As SHREM assured "BTCKing" in a February 27, 2012 e-mail: "I always take care of you, we even know which orders are yours."

38. SHREM even gave "BTCKing" discounts based on the high volume of his transactions with the Company. For example:

a. On May 21, 2012, "BTCKing" wrote to SHREM, stating: "How about giving me discount trades... A lot of cash to BTC goes through my hands as you know, best day yet was 20K to BTC.....if you drop your rates, then I will drop mine and there would then be more volume and more income..." On May 30, 2012, SHREM told "BTCKing" he was willing to give him a "0.50% discount on all orders, and 1% if you hit a certain limit," for them to decide on later.

b. On June 18, 2012, "BTCKing" wrote SHREM, stating that he had a "Possible BIG day" coming up Wednesday - "BIG!!" - and wanted to confirm that he would receive a discount on his orders. SHREM replied, "Ill gladly give you a kickback as promised, no problem. How much do you project?" "BTCKing" stated, "Should be $20-$30k approx."

c. On October 12, 2012, SHREM sent "BTCKing" a spreadsheet summarizing "BTCKing's" orders in August and September 2012, reflecting orders averaging approximately $40,000 per week. SHREM stated, "Do you think you can increase your numbers? I'd be happy to talk about a higher rebate if you can."

## SHREM's Willful Failure to Enforce AML Requirements as to "BTCKing"

39. In addition to generally facilitating "BTCKing's" illegal business, SHREM specifically enabled "BTCKing" to evade AML restrictions imposed by the Company's own AML policy as well as federal law, despite that SHREM himself was responsible for enforcing those restrictions. As explained below, SHREM: regularly permitted "BTCKing" to exceed the Company's AML transaction limits; permitted "BTCKing" to move large amounts of money through the Company without ever identifying himself or his customers, in violation of federal law; and never filed a Suspicious Activity Report concerning "BTCKing," even though he

knew "BTCKing" was operating an underground Bitcoin exchange service on a drug-trafficking website.

40. To begin with, SHREM routinely allowed "BTCKing" to exceed the Company's $1,000 limit on cash deposits per day, imposed pursuant to its AML policy as described in paragraph 20 above, by regularly letting "BTCKing" place multiple orders on a daily basis that, cumulatively, would far exceed $1,000.

41. Even where it was clear that "BTCKing" was submitting orders exceeding $1,000 on behalf of a single customer, SHREM not only condoned these transactions but advised "BTCKing" on how to structure the deposits in order to prevent them from being blocked by the Cash Processor, which checked for deposits exceeding the $1,000 AML limit. For example:

a. On May 12, 2012, "BTCKing" wrote to SHREM to ask whether it was "unacceptable" to make deposits of more than $1,000 at the same bank "in as many deposits as needed," elaborating: "For example...if I want to make a $5000 deposit then I generate 5 deposits on your website and I can go to one bank branch and deposit all the 5 deposits at the same time . . . ?" Based on my experience in this investigation, "BTCKing" was asking whether, if a customer wanted to order $5,000 in Bitcoins from him, "BTCKing" could place five $1,000 orders with the Company and have the customer deposit the money in five corresponding deposits at a single bank branch.

b. SHREM approved of "BTCKing's" proposal, replying that, although the Cash Processor would block any deposit over $1,000 by a single customer at the same bank, the Cash Processor would "assum[e]," based on the five different orders, that "its 5 people making the deposit at one bank branch." SHREM further advised "BTCKing":

> If I were you, I'd spread it out over 2-3 branches to play it safe. It should process fine, but better be safe th[an] sorry. Feel me?

42. As noted in paragraph 20, the reason for the Company's $1,000 cash deposit limit was, in part, so that the Company could avoid ever having to ask its customers for identification. As explained in paragraphs 15.d and 21.d above, pursuant to federal law and the Company's own AML policy, the Company was required to verify the identity of any customer involved in any order or "series of orders" of $3,000 or more - including obtaining the tax identification number of the "paying party" for any order placed on someone else's behalf. By limiting

deposits to $1,000 per day, the Company sought to avoid transactions that would trigger this $3,000 threshold. Yet, as reflected in the previous paragraph, SHREM never asked "BTCKing" for the taxpayer identification numbers of "BTCKing's" customers, even where it was clear that "BTCKing" was placing orders in excess of $3,000 for the same customer. SHREM thereby allowed "BTCKing" to evade not only the Company's daily transaction limit but also its customer verification requirements.

43. SHREM not only permitted "BTCKing's" customers to remain anonymous, but also permitted "BTCKing" himself to do business with the Company anonymously during the entire time they worked together, even though "BTCKing's" orders regularly exceeded $3,000 per day. (Indeed, as indicated in paragraph 38, they sometimes exceeded $20,000 per day.) Again, federal law and the Company's own AML policy required verifying the identity of anyone seeking to transmit more than $3,000 through the Company; yet, as reflected in the exchange below, SHREM deliberately failed to obtain identity documents from "BTCKing":

a. In late July 2013, the Cash Processor CEO sent SHREM several e-mails asking if SHREM had obtained identity documentation for the user "111a@safe-mail.net," based on his high volume of transactions. (As described in paragraph 36.b, above, SHREM knew that e-mail address was being used by "BTCKing" at the time, while the Cash Processor did not.)

b. SHREM replied to the Cash Processor that he was "getting all the info."

c. Subsequently, on August 1, 2013, the following exchange occurred between SHREM and "BTCKing":

i. SHREM wrote to "BTCKing" asking him if he would be willing to supply his "ID and utility bill."

ii. "BTCKing" wrote back: "Charlie, why do you want that. I would rather not have you know anything about anything."

iii. SHREM replied, "If you send it to me, I can raise your [transaction] limits," promising "BTCKing" that he would then "never have problems."

iv. "BTCKing" continued to demur, writing: "C, I'm 52 years old. I am an [e]x business man who was once worth millions… My anonymity is crucial… That is why I pay your fee

otherwise I could set up my own accounts but I feel we have something good going here and I don't want that to change and I don't think you do either." Based on the investigation, I believe "BTCKing" meant that, if it were not for the need to avoid exposing his identity, he would simply have his customers deposit cash into his personal bank accounts, instead of funneling their transactions through the Company and paying the Company's fees as a result.

v. SHREM accepted "BTCKing's" refusal to identify himself, replying, simply, "Ok."

44. Finally, I have checked law enforcement databases to determine whether the Company ever filed any Suspicious Activity Report concerning "BTCKing." Despite "BTCKing's" operation of an underground money transmitting business on an illegal website, his frequent large transactions exceeding the Company's daily deposit limit, and his refusal to validate his identity - all clear signs of suspicious activity and "red flags" under the Company's own AML policies - at no time did SHREM ever file any Suspicious Activity Report with FinCEN concerning "BTCKing."

45. I have reviewed records from the Third Party Exchange for the accounts "BTCKing" used in doing business with the Company, as reflected in various e-mails between "BTCKing" and SHREM. The records show that, during the period from in or about December 2011 through in or about October 2012, approximately $1,050,788 in total was deposited into the accounts, and approximately the same amount was used to purchase Bitcoins. Moreover, I have reviewed bank records for the Company for this time period, which show millions of dollars being wired by the Company to the Third Party Exchange, which would have been used in part to fund the Company's transfers to "BTCKing's" exchange account.[5]

46. Thus, the records indicate that, despite being the Company's AML Compliance Officer, SHREM allowed "BTCKing" to move over $1 million through the Company's system, knowing that the funds would be used to promote "BTCKing's" unlawful Bitcoin exchange service on Silk Road and, ultimately, the drug trafficking on Silk Road that "BTCKing's" business supported.

[5] The wires were sent internationally, from the Company's U.S. bank account to foreign bank accounts maintained by the Third Party Exchange in Japan and Poland.

## "BTCKING'S" CONTINUED OPERATION IN 2013 AFTER PARTING WAYS WITH SHREM

47. Based on contents of the Shrem E-mail Accounts, I know that, on October 27, 2012, the Cash Processor ceased doing business with the Company - in part because, as the Cash Processor CEO told SHREM in an e-mail, SHREM had "not provided an acceptable response to our numerous requests for information" about the Company's "resellers and their clients." As a result, the Company was no longer able to accept cash deposits for Bitcoins. "BTCKing" in turn ceased doing business through the Company at that time.

48. From undercover activity on Silk Road, I know that "BTCKing" temporarily ceased operating on Silk Road after October 2012, presumably due to the loss of the Company's services. "BTCKing" did not resume his operation on Silk Road until April 2013.

49. After "BTCKing" reopened for business, UC-1 again effected undercover transactions with "BTCKing." Those transactions reflect that, upon reopening, "BTCKing" no longer operated his service through the Company, but instead used a personal bank account to receive cash deposits from customers, while imposing new requirements on them due to the resulting increased risk of detection by law enforcement. Specifically:

a. On April 25, 2013, UC-1 attempted to buy Bitcoins from "BTCKing," contacting him through Silk Road's private message system. However, "BTCKing" declined the transaction, stating that UC-1 had to have "at least 8 prior purchases on SR" to do business with him. Based on my experience in the investigation, I believe "BTCKing" adopted this rule to help ensure his customers were bona fide Silk Road users, as opposed to undercover law enforcement agents.

b. On May 28, 2013, UC-1 again attempted to purchase Bitcoins from "BTCKing," this time using an undercover Silk Road account that had previously been used to make more than eight undercover purchases of drugs on Silk Road (as reflected in the transactional history for the account, visible to other Silk Road users such as "BTCKing"). In placing the order, UC-1 told "BTCKing" that UC-1 needed "about $3000 of bit coins to cover the cost of some fine imported coke I had my eye on."

c. "BTCKing" responded later that day, telling UC-1 to deposit "EXACTLY $3320.00 [CASH ONLY]" into a bank account

held in the name of "R M Faiella," and providing the bank and account number. UC-1 made the deposit the next day.

d. UC-1 subsequently received a confirmation message from "BTCKing" indicating that the deposit had been received and that UC-1 should soon receive $3320 in Bitcoins (less "BTCKing's" nine-percent fee). UC-1 checked UC-1's Silk Road account several hours later and saw that the Bitcoins had been credited to UC-1's Silk Road Bitcoin address.

50. Other evidence reflects that "BTCKing" was able to resume a high volume of business operating in this fashion. Among other things, I have reviewed data from computer servers used to host the Silk Road website, which were imaged by law enforcement in the course of investigating Silk Road. The server data includes the messages sent to and from "BTCKing" through Silk Road's private message system, which reflect numerous Bitcoin exchange transactions consummated with other Silk Road users. From May 1, 2013 to June 30, 2013, for example, "BTCKing's" private messages reflect exchange transactions averaging approximately $20,000 per week. By September 2013, the messages reflect that he was averaging approximately $25,000 per week. As to nearly all of the transactions reflected in his private messages, the messages reflect that "BTCKing" had his customers deposit funds into the bank account referenced in paragraph 49.b, held in the name of "R M Faiella." As to a handful of other orders, "BTCKing" instructed his customers to send cash through the mail to "RMF Trust Co." at a post office box located in Cape Coral, Florida.

51. "BTCKing's" private messages in 2013 further reflect a continuing awareness of the illegal nature of his business, and a continuing effort to evade detection by law enforcement. In particular, on June 15, 2013, "BTCKing" announced to his customers that he was now operating in "stealth mode" in order to "keep[] the outsiders out." According to the Silk Road website, vendors on the site who considered themselves at particular "risk of becoming a target for law enforcement" could operate in "stealth mode," meaning that the vendor's listings were not visible to users searching or browsing the site. Instead, only users who already knew the specific address of the vendor's homepage on Silk Road were able to access the vendor's offerings. In this way, the vendor was thought to be insulated from undercover law enforcement agents operating on the site.

52. "BTCKing's" private messages further reflect that "BTCKing" was specifically aware that he was operating an unlicensed money transmitting business. In particular, from

July 30, 2013 to August 1, 2013, "BTCKing" had an extended exchange with the owner and operator of the Silk Road site, known by the Silk Road username "Dread Pirate Roberts," or "DPR."[6] In the exchange, in sum and substance, "DPR" stated that he was interested in establishing an "Anonymous Bitcoin Exchange," separate from Silk Road, where he wanted to move the "best exchangers" currently operating on Silk Road. "DPR" explained that the new site would be specifically tailored to Bitcoin exchange services, and that he would personally "supply liquidity" to the exchangers on the site. "BTCKing's" feedback on "DPR's" proposal reveals that he fully understood his business was illegal:

a. "BTCKing" told "DPR" that that there would have to be a way on the "Anonymous Bitcoin Exchange" for him to "deal only with veteran SR [Silk Road] members" given that "LE [law enforcement] will be all over this at first."

b. "BTCKing" elaborated that a Bitcoin exchange business was considered a "MSB" (money services business) and had "to be licensed."

c. "BTCKing" explained to "DPR," in sum and substance, that if his business was investigated, it would be easy for law enforcement to identify him given that he was using personal bank accounts to conduct transactions, stating:

> All LE has to do is go to the bank and ask who is the Trustee of RMF Trust and BANG... They will seize the funds and me. These organizations are IRS, Treasury Dept, FINCEN, Dept of Justice, Global illicit Financial Team, US Secret Service, Homeland security... All of these have seized Liberty Reserve...[7]

d. "BTCKing" noted he was already having trouble with "a couple of banks that live and love the BSA [Bank Secrecy Act]," as he was having to convince the banks to allow regular cash deposits into his account and outgoing wires to the Third

---

[6] A separate complaint filed in this district on September 27, 2013, charges that the "Dread Pirate Roberts" username was controlled by ROSS WILLIAM ULBRICHT, a/k/a "Silk Road," a/k/a "Dread Pirate Roberts," a/k/a "DPR," who the complaint alleges to have been the owner and operator of the site.

[7] Liberty Reserve was a virtual currency service seized by the Government in May 2013 based on charges of money laundering and operating an unlicensed money transmitting business.

Party Exchange. "BTCKing" added that he had told the banks he was operating a "private peer to peer investment group."

e. In light of all of these concerns, "BTCKing" told "DPR" that he did not want to participate in the proposed "Anonymous Bitcoin Exchange" and preferred instead to continue operating on Silk Road in "stealth mode."

53. Based on undercover activity on Silk Road, I know that "BTCKing" continued operating on Silk Road until the site was seized by law enforcement authorities on October 2, 2013.

54. From reviewing FinCEN records, I know that no business under the name of "BTCKing" or "Robert M. Faiella" has ever registered as a money services business with FinCEN.

## IDENTIFICATION OF "BTCKING" AS ROBERT M. FAIELLA

55. As described above in paragraphs 49.b and 50, after reopening his service on Silk Road in April 2013, "BTCKing" consistently told his customers to deposit their funds into a bank account held by "R M Faiella." I have reviewed records for the account in question, which reflect that ROBERT M. FAIELLA, the defendant, is the lone signatory on the account, and that he opened the account in October 2012 in Florida, around the same time that the Company ceased accepting cash deposits.

56. I have also reviewed records from the Third Party Exchange relating to the accounts there that "BTCKing" used to receive funds from the Company. The records reflect that the Third Party Exchange had required the customer to submit identity documents to maintain the accounts, and that the identity documents submitted were in the name of ROBERT M. FAIELLA, the defendant.

57. Further, as described in paragraph 27, in numerous e-mails originating from "BTCKing's" various e-mail accounts, "BTCKing" signed his e-mails with the letter "B." Additionally, at least two e-mails were signed with the name "Bob."

58. Similarly, as referenced in paragraph 43.c.iv, in an e-mail sent to SHREM, "BTCKing" mentioned he was "52 years old." This matches the age of ROBERT M. FAIELLA, the defendant.

59. I have also examined the headers of many of the e-mails sent by "BTCKing," many of which reflect a particular IP address for the sender of the e-mail. According to records from the Internet service provider that controls the IP address, the

IP address was assigned at the relevant times to a woman known to be the wife of ROBERT M. FAIELLA, the defendant, at an address in Cape Coral, Florida, known to be FAIELLA's home address. Further, from reviewing "BTCKing's" e-mail communications with SHREM, I know that, in an e-mail dated May 24, 2012, "BTCKing" told SHREM he lived in south Florida.

60. Accordingly, I believe that the individual responsible for operating an underground Bitcoin exchange service on Silk Road as "BTCKing," with the assistance of CHARLIE SHREM, the defendant, is ROBERT M. FAIELLA, a/k/a "BTCKing," the defendant.

WHEREFORE, I respectfully request that arrest warrants be issued for ROBERT M. FAIELLA, a/k/a "BTCKing," and CHARLIE SHREM, the defendants, and that they be arrested and imprisoned or bailed, as the case may be.

GARY L. ALFORD
Special Agent
Internal Revenue Service

Sworn to before me this
24th day of January 2013

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK