

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INDEX OF EXHIBITS

United States v. Thomas Mario Costanzo

CR-17-585-PHX-GMS

Exhibit L Lord Indictment, CR-15-240-SMH (W.D. La.)

Exhibit M Lord Memorandum Ruling

Exhibit N Lord Sentencing Minutes

Exhibit O Faiella, et al. Complaint

Exhibit P Shrem Judgement & Commitment

Exhibit Q Faiella Judgment & Conviction

Exhibit R *Bitcoin crime nets prison time for Pa. heroin trafficker*

EXHIBIT

L

RECEIVED

NOV 18 2015

TONY R. MOORE, CLERK
WESTERN DISTRICT OF LOUISIANA
SHREVEPORT, LOUISIANA

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
SHREVEPORT DIVISION

| | | | |
|--------------------------|-------|--------------------------------------|----------------------|
| UNITED STATES OF AMERICA | * | CRIMINAL NO.: | <u>5:15-cr-00240</u> |
| | * | | |
| | * | 18 U.S.C. §§ 1960, 1956(a)(3)(B)-(C) | |
| | * | 18 U.S.C. §§ 1843, 2 | |
| | * | 31 U.S.C. §§ 5313, 5322 | |
| VERSUS | * | 21 U.S.C. § 846 | |
| | * | 18 U.S.C. § 982 | |
| | * | | |
| | * | | |
| MICHAEL A. LORD | (1) * | JUDGE | <u>Hicks</u> |
| RANDALL B. LORD | (2) * | MAGISTRATE JUDGE | HORNSBY |

INDICTMENT

THE GRAND JURY CHARGES:

COUNT 1

18 U.S.C. § 371

(Conspiracy to Operate an Unlicensed MSB)

I. AT ALL TIMES RELEVANT HEREIN:

A. BITCOIN BACKGROUND

1. The Defendants, MICHAEL A. LORD and RANDALL B. LORD, have been in the bitcoin exchange business since at least 2013. The Defendants initially used their personal checking accounts in connection with their bitcoin business. Then the Defendants established and used the following companies to facilitate the sale and transfer of bitcoin:

a. MICHAEL A. LORD has been doing business as (dba)

Crypto Processing Solutions since approximately November 2013.

b. **RANDALL B. LORD** has been dba as Quantum Health since on or about August 2014.

c. **RANDALL B. LORD** incorporated Data Security LLC and Pelican Mining LLC in the State of Nevada on or about August 13, 2014.

d. **RANDALL B. LORD** was a chiropractor by training. His license expired on or about December 31, 2007. **RANDALL B. LORD** had various bank accounts titled in the name of Jewella Chiropractic Clinic.

2. Bitcoin are a decentralized form of electronic or digital 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 “peer-to-peer” network. An individual can send and receive bitcoin through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

3. To acquire bitcoin, a user typically must purchase them from a bitcoin “exchanger.” In return for a commission, bitcoin exchangers accept payments of currency in some conventional form (e.g., cash, wire transfer, etc.) and exchange the money for bitcoin based on a fluctuating exchange rate.

4. Once a user acquires bitcoin from an exchanger, the bitcoin are stored on digital “wallets” associated with a bitcoin “address.” A bitcoin wallet is what allows a user to transact with other users. It gives a user ownership of bitcoin balances so a user can send and receive bitcoin.

5. Only if one knows the identities associated with each bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system. Bitcoin transactions are, therefore, described as “pseudonymous,” meaning they are partially anonymous.

B. MONEY TRANSMITTING LAWS

1. The federal unlicensed money transmitting business statute, Title 18, United States Code, Section 1960, was enacted in 1992 in order to combat the growing use of money transmitting businesses to transfer large amounts of the monetary proceeds of unlawful enterprises.

2. Financial institutions are defined in the Code of Federal Regulations as “money servicing businesses,” (“MSBs”) which include money transmitters. Money transmitting is defined as “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”

3. MSBs are subject to the provisions of the Bank Secrecy Act. The Bank Secrecy Act and its implementing regulations require, among other things, MSBs to take steps to avoid laundering the proceeds of crime and to report suspicious transactions to law enforcement authorities. Unlike an ordinary business, MSBs have an independent statutory and regulatory obligation to understand the nature and source of the funds they transmit, and to ensure systems are in place to detect and prevent transactions made with the proceeds of

crime.

4. It is a violation of federal law to operate an MSB without the appropriate state license and federal registration, or when it otherwise involves the transportation or transmission of funds that are known to have been derived from a criminal offense or intended to be used to promote unlawful activity. MSBs are required to register with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of Treasury within 180 days after the date the business is established.

5. Bitcoin exchangers such as the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, and their companies are MSBs subject to federal and state laws and regulations.

C. THE CONSPIRACY

From at least in or about 2013 through on or about the present, the exact dates being uncertain, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, unlawfully, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, to conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business in violation of Title 18, United States Code, Section 1960.

D. THE OBJECT OF THE CONSPIRACY

It was a part and an object of the conspiracy for the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, to operate an unlicensed MSB and improperly

obtain funds.

E. MEANS AND METHODS OF THE CONSPIRACY

Among the means and methods by which the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, would and did carry out the conspiracy were the following:

1. The Defendant, **MICHAEL A. LORD**, advertised bitcoin services via the internet at <https://localbitcoins.com> under the username Internet151.

2. The Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, solicited, accepted and made deposits of quantities of currency and other monetary instruments, including money paks and money orders, into their personal and business bank accounts. The total value of the deposits made and accepted was more than \$3,500,000.

3. The currency and monetary value accepted by the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, was transferred from their various bank accounts to a virtual currency exchange service which converted the currencies into bitcoin.

4. During the period relevant to this Indictment, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, and their companies did not obtain licenses to engage in the business of money transmission by the State of Louisiana.

5. Between 2013 and November 10, 2014, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, and their companies did not register as a money transmitting business with the United States Treasury Department. From November 10, 2014 to the present, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, and their companies, Crypto Processing Solutions, Quantum Health and Data Security, LLC, did not register as a money transmitting business with FinCEN.

F. OVERT ACTS

1. In furtherance of the conspiracy and to affect the illegal object thereof, the following overt acts, among others, were committed in the Western District of Louisiana and elsewhere:

a. Between on or about April 11, 2014 and April 14, 2014, the Defendant, **MICHAEL A. LORD**, accepted and made cash deposits from third parties into his Wells Fargo Bank, N.A. account ending in -3621 and which were followed by ACH withdrawals by a virtual currency exchanger to purchase bitcoin:

i. \$5,500 in cash deposited on April 11, 2014 followed by a \$5,499.99 virtual currency exchange transaction on April 14, 2014. On April 11, 2014, 12.852 bitcoin were purchased for \$5,499.99;

ii. \$1,900 in cash deposited on April 11, 2014 followed by a \$1,900.01 virtual currency exchange transaction on April 14, 2014. On April 14, 2014, 4.132 bitcoin were purchased for \$1,893.55; and

iii. \$1,780 in cash deposited on April 11, 2014 followed by a \$1,779.99 virtual currency exchange transaction on April 14, 2014. On April 11, 2014, 3.308 bitcoin were purchased for \$1,500.09.

b. Between on or about March 31, 2014 and April 1, 2014, the Defendant, **RANDALL B. LORD**, accepted and made cash deposits and money orders from third parties into his Wells Fargo Bank, N.A. account for Quantum Health ending in -7772 and which were followed by ACH withdrawals by a virtual currency exchanger to purchase bitcoin:

i. \$1,950 in cash deposited on March 31, 2014 followed by a \$1,949.99 virtual currency exchange transaction on April 1, 2014. On April 4, 2014, 4.2251 bitcoin were purchased for \$1,949.99; and

ii. \$1,856.65 in money orders deposited on March 31, 2014 followed by a \$1,856.62 virtual currency exchange transaction on April 1, 2014. On April 4, 2014, 3.6905 bitcoin were purchased for \$1,856.62.

2. The allegations contained in Count 2 are re-alleged and incorporated by reference as though set forth in full herein as additional overt acts, all in violation of Title 18, United States Code, Section 371. [Title 18, United States Code, Section 371].

COUNT 2

18 U.S.C. §§ 1960(a), (b)(1)-(2) & 18 U.S.C. § 2
(Unlicensed Money Service Business)

From at least in or about 2013 through on or about the present, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD**

and **RANDALL B. LORD**, unlawfully, willfully, and knowingly conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, (a) without an appropriate money transmitting license, and (b) while failing to comply with the money transmitting business registration requirements under Title 31, United States Code, Section 5220 and regulations prescribed under such section, to wit, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, transmitted millions of dollars by means including cash, money orders and electronic transfers to and through Louisiana and elsewhere without registering as a money transmitting business under federal law and without obtaining a Louisiana money transmitting license, all in violation of Title 18, United States Code, Sections 1960(a), (b)(1)-(2) and 18 U.S.C. § 2. [18 U.S.C. §§ 1960(a), (b)(1)-(2) & 18 U.S.C. § 2].

COUNT 3

18 U.S.C. §§ 1956(a)(3)(B) & 18 U.S.C. § 2
(Money Laundering)

On or about February 4, 2015, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly conduct and attempt to conduct a financial transaction affecting interstate commerce, that is, the exchange of \$14,000 in U.S. currency for bitcoin, involving property represented by a person acting at the direction of a federal official to be proceeds of a specified unlawful activity, i.e., the distribution of controlled substances, with the intent to conceal and disguise the nature, source,

ownership, and control of such property, all in violation of Title 18, United States Code, Sections 1956(a)(3)(B) and 2. [18 U.S.C. § 1956(a)(3)(B) and 18 U.S.C. § 2].

COUNT 4

18 U.S.C. §§ 1956(a)(3)(C) & 18 U.S.C. § 2
(Money Laundering)

On or about February 4, 2015, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly conduct and attempt to conduct a financial transaction affecting interstate commerce, that is, the exchange of \$14,000 in U.S. currency for bitcoin, involving property represented by a person acting at the direction of a federal official to be proceeds of a specified unlawful activity, i.e., the distribution of controlled substances, with the intent to avoid a reporting requirement under federal and state law, by structuring the bank deposit of a portion of the \$14,000 in U.S. currency received in one transaction, all in violation of Title 18, United States Code, Sections 1956(a)(3)(C) and 2. [18 U.S.C. § 1956(a)(3)(C) and 18 U.S.C. § 2].

COUNT 5

31 U.S.C. §§ 5313, 5322 & 18 U.S.C. § 2
(Failure to File CTRs)

A. When a domestic financial institution is involved in a transaction for the deposit, withdrawal, exchange of currency, or other payment or transfer, of United States coins or currency in an amount greater than \$10,000, the domestic financial institution shall file a Currency Transaction Report ("CTR") with respect to such transaction or transactions with the Financial Crimes Enforcement Network (FinCEN) within 15 days of the reportable cash transaction. 31 U.S.C. §

5331(a). The CTR must contain the name, address and taxpayer information of the person from whom the cash was received and the amount of cash deposited, withdrawn, exchanged for currency, or other payment or transfer.

B. On or about February 19, 2015, in the Western District of Louisiana, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly and willfully fail to file a Currency Transaction Report as required under Title 31, United States Code, Section 5313 and any regulation prescribed under any such section, all in violation of Title 31, United States Code, Sections 5313 and 5322 and Title 31, Code of Federal Regulations, Part 103, recodified as Title 31, Code of Federal Regulations, Chapter X (effective March 1, 2011) and Title 18, United States Code, Section 2. [31 U.S.C. §§ 5313, 5322 and 18 U.S.C. § 2].

COUNT 6

18 U.S.C. §§ 1956(a)(3)(B) & 18 U.S.C. § 2
(Money Laundering)

On or about February 24, 2015, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly conduct and attempt to conduct a financial transaction affecting interstate commerce, that is, the exchange of \$19,000 in U.S. currency for bitcoin, involving property represented by a person acting at the direction of a federal official to be proceeds of a specified unlawful activity, i.e., the distribution of controlled substances, with the intent to conceal and disguise the nature, source, ownership, and control of such property, all in violation of Title 18, United States Code, Sections 1956(a)(3)(B) and 2. [18 U.S.C. § 1956(a)(3)(B) and 18 U.S.C. § 2].

COUNT 7

18 U.S.C. §§ 1956(a)(3)(C) & 18 U.S.C. § 2
(Money Laundering)

On or about February 24, 2015, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly conduct and attempt to conduct a financial transaction affecting interstate commerce, that is, the exchange of \$19,000 in U.S. currency for bitcoin, involving property represented by a person acting at the direction of a federal official to be proceeds of a specified unlawful activity, i.e., the distribution of controlled substances, with the intent to conceal and disguise the nature, source, ownership, and control of such property, and with the intent to avoid a reporting requirement under federal and state law, by structuring the bank deposit of a portion of the \$19,000 in U.S. currency received in one transaction, all in violation of Title 18, United States Code, Sections 1956(a)(3)(C) and 2. [18 U.S.C. § 1956(a)(3)(C) and 18 U.S.C. § 2].

COUNT 8

31 U.S.C. §§ 5313, 5322 & 18 U.S.C. § 2
(Failure to File CTRs)

A. The allegations of Count 5 paragraph A are re-alleged and incorporated by reference as though set forth in full herein.

B. On or about March 11, 2015, in the Western District of Louisiana, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, did knowingly and willfully fail to file a Currency Transaction Report as required under Title 31, United States Code, Section 5313 and any regulation prescribed under any such

section, all in violation of Title 31, United States Code, Sections 5313 and 5322 and Title 31, Code of Federal Regulations, Part 103, recodified as Title 31, Code of Federal Regulations, Chapter X (effective March 1, 2011) and Title 18, United States Code, Section 2. [31 U.S.C. §§ 5313, 5322 and 18 U.S.C. § 2].

COUNTS 9-14
18 U.S.C. §§ 1343 & 18 U.S.C. § 2
(Wire Fraud)

A. BACKGROUND

1. The allegations contained in Count 1 including subparagraphs are re-alleged and incorporated by reference as though set forth in full herein.

2. The Defendants utilized a number of Card Processors in connection with their bitcoin business including the following:

a. Chase Paymentech a credit and debit card processor associated with JPMorgan Chase Bank, N.A.

b. Merchant One, Inc. a credit and debit card processor associated with Wells Fargo Bank, N.A.

c. National Processing Company ("NPC") and PaySimple credit and debit card processors associated with Fifth Third Bank.

d. TransFirst, LLC a credit and debit card processor associated with Synovus Bank dba Columbus Bank and Trust Company and with Wells Fargo Bank, N.A.

3. The Card Processors classified bitcoin related businesses as high-risk subject to particularized underwriting or excluded such merchants altogether.

B. THE SCHEME AND ARTIFICE TO DEFRAUD

The primary object of the scheme and artifice to defraud was to conceal the true nature of the business conducted under the name Jewella Chiropractic Clinic and Quantum Health and thereby obtain the ability to process credit and debit cards when exchanging bitcoin for currency and funds.

C. MANNER AND MEANS OF ACCOMPLISHING THE SCHEME AND ARTIFICE TO DEFRAUD

1. Beginning in May 2014 and continuing until July 2015, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, for the purpose of executing and attempting to execute the aforesaid scheme and artifice to defraud the Card Processors, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, did knowingly cause to be transmitted by means of a wire communication in interstate commerce the writings, signs, signals, pictures, and sounds.

2. It was part of the scheme and artifice to defraud that the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, submitted applications to the above-listed Card Processors that misrepresented their business activities.

a. On or about May 23, 2014, the Defendant, **RANDALL B. LORD**, submitted a merchant application to Chase Paymentech and described his business as Jewella Chiropractic Clinic. After being approved by Chase Paymentech, approximately \$117,000 in transactions were processed and payments were sent to a JPMorgan Chase Bank, N.A. account titled Jewella Chiropractic Clinic. The descriptions associated with the card transactions were mislabeled (such as chakra realignment, mood counseling, spiritual tuneup, karama cleansing, etc.) to conceal the actual purpose of the transaction, which was to purchase bitcoin with funds from the credit and debit cards.

b. On or about August 14, 2014, the Defendant, **RANDALL B. LORD**, submitted a merchant application to Merchant One and falsely described his business as Quantum Health, a health clinic. A pamphlet submitted with the application falsely stated that Quantum Health was providing energy medicine to conceal the actual purpose of the business, which was to purchase bitcoin with funds from the credit and debit cards. After being approved by Merchant One, approximately \$2,232 in transactions were processed and payments were sent to a Regions Bank account titled Quantum Health.

c. On or about November 12, 2014, the Defendant, **RANDALL B. LORD**, submitted a merchant application to PaySimple/NPC and falsely described his business as Quantum Health, a health services and chiropractic business to conceal the actual purpose of the business, which was to purchase bitcoin with funds from the credit and debit cards. After being approved

by PaySimple/NPC, approximately \$162,155 in transactions were processed and payments were sent to a Ouachita Independent Bank account titled Quantum Health.

d. On or about December 2, 2014, the Defendant, **RANDALL B. LORD**, submitted a merchant application to TransFirst and falsely described his business Quantum Health, as a medical services company to conceal the actual purpose of the business, which was to purchase bitcoin with funds from the credit and debit cards. Payments were authorized to be processed into an Ouachita Independent Bank account titled Quantum Health. After being approved by TransFirst, Quantum Health was subjected to an underwriting review. On or about April 30, 2015, the Defendant, **RANDALL B. LORD**, submitted another merchant application to TransFirst.

3. It was further part of the scheme and artifice to defraud that the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, created false invoices for services to further mislead the Card Processors about their actual business activities.

4. On or about each of the dates set forth below, in the Western District of Louisiana and elsewhere, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, for the purpose of executing and attempting to execute the aforesaid scheme and artifice to defraud the Card Processors, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, did knowingly cause to be transmitted by means of a

wire communication in interstate commerce the writings, signs, signals, pictures, and sounds described below for each count between Shreveport, Louisiana and other states, that is, electronic submission of the below described documents to the Card Processors:

| Count | Date of Wire Communication | Card Processor | Description |
|-------|----------------------------|------------------|--|
| 9. | 5/23/2014 | Chase Paymentech | Merchant application submitted to Chase Paymentech |
| 10. | 8/14/2014 | Merchant One | Merchant application submitted to Merchant One |
| 11. | 11/12/2014 | PaySimple/NPC | Merchant application submitted to PaySimple/NPC |
| 12. | 12/2/2014 | TransFirst | Merchant application submitted to TransFirst |
| 13. | 12/4/2014 | TransFirst | Quantum Health invoice dated 12/3/2014 submitted to TransFirst |
| 14. | 4/30/2015 | TransFirst | Merchant application submitted to TransFirst |

all in violation of Title 18, United States Code, Sections 1343 and 2. [18 U.S.C. §§ 1343 and 2].

COUNT 15
(21 U.S.C. § 846)
Drug Conspiracy

Beginning approximately March 2015, and continuing through on or about the present, the exact dates being unknown, in the Western District of Louisiana and elsewhere, the Defendant, **MICHAEL A. LORD**, and other persons known and unknown to the Grand Jury, did knowingly and intentionally conspire and agree together to distribute and to possess with the intent to distribute controlled dangerous substances to include Alprazolam, a Schedule IV controlled substance, in

violation of Title 21, United States Code, Sections 841(a)(1), (b)(1)(C) and 846, all in violation of Title 21, United States Code, Sections 841(a)(1) and 846. [21 U.S.C. §§ 841(a)(1) and 846].

FORFEITURE ALLEGATION

1. The allegations in Counts 1-4, and 6-7 of this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(1) and Title 21, United States Code, Section 853.

2. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of an offense, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, shall forfeit to the United States of America any property, real or personal, involved in the offense or traceable to such property.

3. The allegations in Counts 9-14 of this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2) and Title 21, United States Code, Section 853.

4. Pursuant to Title 18, United States Code, Section 982(a)(2), upon conviction of an offense, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, shall forfeit to the United States of America any property constituting or derived from proceeds the Defendants obtained directly or indirectly as the result of said violations as set forth in this Indictment.

5. The allegations in Counts 5 and 8 of this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 31, United States Code, Section 5317(c)(1).

6. Pursuant to Title 31, United States Code, Section 5317, upon conviction of an offense in violation of Title 31, United States Code, Sections 5313 and 5322, the Defendants, **MICHAEL A. LORD** and **RANDALL B. LORD**, shall forfeit to the United States of America all property, real or personal, involved in the offense alleged in Counts 5 and 8, and any property traceable thereto.

7. The allegations in Count 15 are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to the provisions of Title 21, United States Code, Section 853, Rule 32.2(a) of the Federal Rules of Criminal Procedure.

8. Upon conviction of the controlled substances offense alleged in Count 15, the Defendant, **MICHAEL A. LORD**, shall forfeit to the United States all of his interest in:

a. Any property consisting or derived from proceeds the Defendant obtained directly or indirectly as the result of said violations as set forth in this Indictment and,

b. Any property used or intended to be used in any manner or part to commit or facilitate the commission of the aforementioned violations.

9. If any of the property described above, as a result of any act or omission of the Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

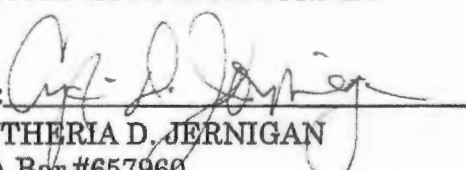
the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, 981(b)(1) and Title 28, United States Code, Section 2461(c).

A TRUE BILL:

REDACTED

GRAND JURY FOREPERSON

STEPHANIE A. FINLEY
UNITED STATES ATTORNEY

By: 
CYTHERIA D. JERNIGAN
MA Bar #657960
Assistant United States Attorney
300 Fannin Street, Suite 3201
Shreveport, LA 71101
(318) 676-3600 – office
(318) 676-3663 – fax

EXHIBIT

M

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
SHREVEPORT DIVISION**

UNITED STATES OF AMERICA

CRIMINAL ACTION NO. 15-00240-
01/02

VERSUS

JUDGE S. MAURICE HICKS, JR.

MICHAEL A. LORD AND
RANDALL B. LORD

MAGISTRATE JUDGE HORNSBY

MEMORANDUM RULING

Before the Court is Defendants Michael A. Lord (“Michael Lord”) and Randall B. Lord’s (“Randall Lord”) (collectively “Defendants”) Motion to Withdraw their guilty pleas (Record Document 51). The Government opposes Defendants’ Motion. See Record Document 54. For the reasons contained in the instant Memorandum Ruling, Defendants’ Motion is **DENIED**.

FACTUAL AND PROCEDURAL BACKGROUND

Randall Lord is a former chiropractor and resident of Shreveport, Louisiana. See Record Document 1. Michael Lord is Randall Lord’s son, and he lives with his father in Shreveport. See id. Beginning in 2013, Defendants began operating a business in which they exchanged cash, credit card payments, and other forms of payment for bitcoins. See Record Document 42 at 11-13 (guilty plea hearing testimony of Darrin Heusel, IRS Criminal Investigations Division). The bitcoin is a decentralized form of online currency that is maintained in an online “wallet.” See id. Bitcoins can be purchased from online exchangers or brokers, who often charge a fee for making such an exchange. See id. Bitcoins can then be exchanged for other goods or services online and transferred to another person’s wallet. See id. That person can then either use such bitcoins to

purchase other goods and services or convert them back to U.S. dollars or some other traditional form of currency. See id.

Defendants operated their bitcoin business through a website called localbitcoins.com, on which they posted advertisements for bitcoin exchange services. See id. at 14. Persons who engaged Defendants' services would transfer money to Defendants by some traditional means, such as cash or wire transfer. See id. Then, Defendants would purchase bitcoins from Coinbase, another online bitcoin broker, and transfer the bitcoins back to the buyer after subtracting their commission. See id. Though Defendants initially used personal bank accounts for these transactions, they eventually used accounts associated with the following: (1) Randall Lord's former chiropractic clinic, Jewella Chiropractic Clinic; (2) two "doing business as" designations, Crypto Processing Solutions and Quantum Health; and (3) two newly-formed Nevada limited liability companies, Data Security LLC and Pelican Mining LLC. See id. at 12; see Record Document 1 at ¶ 1.

At some point in the spring of 2014, Coinbase contacted Defendants regarding the volume of activity that had been occurring in their account and its consequences. See Record Document 42 at 15-16. Coinbase informed Defendants that because they were acting as bitcoin exchangers they were required to register with the Federal Crimes Enforcement Network ("FinCEN"), a division of the Department of the Treasury, under March 2013 guidance from FinCEN that clarified that bitcoin exchangers were subject to registration requirements. See id. In July 2014, Defendants represented to Coinbase that they were registered with FinCEN, though they were not registered with FinCEN at that time. See id. Defendants did not register with FinCEN until November

2014. See id. By that time, Defendants' bitcoin business had exchanged more than \$2.5 million for bitcoins for customers all around the United States. See id. at 15-17. Defendants continued operating the bitcoin exchange business through 2015. See id. at 11-25.

At the same time, Michael Lord became involved in a drug conspiracy. See id. at 27-40 (guilty plea testimony of Richard Brian Upchurch, Department of Homeland Security Investigations Division). Evidently, Randall Lord was not involved in this separate conspiracy. See id. In May 2015, agents of the Department of Homeland Security in San Francisco intercepted a package from China that contained approximately one kilogram of 5F-AB-PINACA, a synthetic cannabinoid that is a controlled substance. See id. at 27-28. The package was addressed to 711 Seventh Street, Springhill, Louisiana. See id. at 28. On May 18, 2015, the Department of Homeland Security conducted a controlled delivery of the package to that address and subsequently arrested Al Hasnat Langhari ("Langhari") in connection with receiving the package. See id.

While discussing this package and other matters in an interview with Homeland Security agents, Langhari stated that he had been a customer of Defendants' bitcoin exchange business on localbitcoins.com, and that he had come to know and trust Michael Lord after several exchanges. See id. at 29. Langhari stated that he and Michael Lord had decided to start a business for the distribution of Xanax, a commercial name for the Schedule IV controlled substance alprazolam, and use the "darknet" website Agora to set up this business. See id. To start this business, they had acquired a pill press, a binding agent to be mixed with alprazolam, a powder containing

alprazolam itself, and a metal part called a “Xanax die.” See id. at 29-32. Agents either intercepted these materials in the mail or found all of these materials during a search of a business owned by Langhari’s father in southern Arkansas. See id.

After Langhari’s arrest, he contacted his girlfriend, Michell Duhé, a student at Louisiana State University in Baton Rouge. See id. at 35-36. He convinced her and several friends of hers to sell what was described as 10,000 Xanax pills to attempt to raise bail money for Langhari. See id. However, the pills were in north Louisiana, and needed to be taken to south Louisiana to be sold. See id. Michael Lord took the pills to south Louisiana and delivered them to a friend of Duhé’s, Zach Bajat (“Bajat”). See id. at 36-37. In a subsequent interview with federal agents, Bajat was able to identify Michael Lord out of a six-person lineup as the person who delivered the pills to him. See id. at 37. Michael Lord later denied involvement in this drug conspiracy when interviewed by federal agents in July 2015. See id. at 37-38.

On November 18, 2015, a federal grand jury for the Western District of Louisiana issued a 15-count indictment against Defendants. See Record Document 1. Count 1 of the indictment charged Defendants with conspiracy to operate an unlicensed money service business in violation of 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 1960 (unlicensed money transmitting businesses). See id. at 1-3. Counts 2-14 charged Defendants with various other crimes associated with operating their bitcoin exchange business. See id. at 7-16. Count 15 charged Michael Lord with being a member of a drug conspiracy in violation of 21 U.S.C. § 846, 841(a)(1), and (b)(1)(C). See id. at 17. On April 19, 2016, Defendants appeared before this Court and pleaded guilty to Count 1 of the indictment and Michael Lord pleaded guilty to Count 15 of the indictment pursuant

to a plea agreement with the Government. See Record Documents 31, 34, and 35. Defendants filed the instant Motion to Withdraw their guilty pleas on February 21, 2017. See Record Document 51. The Government opposes the Motion, and the Motion is fully briefed. See Record Documents 54 and 57.

LAW AND ANALYSIS

I. Legal Standards

Federal Rule of Criminal Procedure 11(d)(2)(B) states that a criminal defendant may withdraw a plea of guilty after the court accepts the plea but before the imposition of a sentence when “the defendant can show a fair and just reason for requesting the withdrawal.” Thus, a defendant “does not have an absolute right to withdraw a plea,” and a defendant bears the burden of persuading the Court that the reason advanced for withdrawal is “fair and just.” United States v. Conroy, 567 F.3d 174, 177 (5th Cir. 2009); Fed. R. Crim. P. 11(d)(2)(B). A district court has discretion to grant or deny such a motion, and a district court’s decision on such a motion is reviewed for an abuse of discretion. See Conroy, 567 F.3d at 177.

In deciding a motion to withdraw a guilty plea, the Court must consider the following factors:

(1) whether or not the defendant has asserted his innocence; (2) whether or not the government would suffer prejudice if the withdrawal motion were granted; (3) whether or not the defendant has delayed in filing his withdrawal motion; (4) whether or not the withdrawal would substantially inconvenience the court; (5) whether or not close assistance of counsel was available; (6) whether or not the original plea was knowing and voluntary; and (7) whether or not the withdrawal would waste judicial resources.

Id. at 178. This factor-based test is a “totality of the circumstances” test in which “no single factor or combination of factors mandates a particular result.” Id.

II. Analysis

The parties' arguments center on the first factor that must be considered in deciding a motion to withdraw a guilty plea, whether Defendants have asserted their innocence. See Record Documents 51-1, 54, and 57. Defendants argue that they "have always believed that their buying and selling of bitcoins did not make them a money services business ("MSB") and therefore, they were not required to obtain a license to operate their business." Record Document 51-1 at 2. Defendants also argue that they have now confirmed with the State of Louisiana's Office of Financial Institutions ("OFS") that the State of Louisiana does not require a license for persons to engage in exchanging or brokering bitcoins. See id. at 2-3.

The Government concedes that Defendants were not required to obtain an MSB license from the State of Louisiana to operate such a business. See Record Document 54 at 12. However, the Government argues that this concession is not fatal to the charges against Defendants in Count 1 of the indictment because the failure to obtain a state license was but one theory upon which Count 1 is based. See id. The Government also argues that most of the other factors that must be considered weigh in favor of denying the Motion. See id. at 11-17. Defendants devote no argument to whether Michael Lord should be allowed to withdraw his guilty plea to Count 15 of the indictment for his role in a drug conspiracy. See Record Documents 51-1 and 57.

A. Defendants May Not Withdraw Their Guilty Pleas to Count 1.

The Government's argument on the first factor, whether Defendants have asserted their innocence, is correct. Defendants correctly argue, and the Government has conceded, that the fact that the State of Louisiana does not require a license to

operate an MSB precludes one theory upon which Count 1 of the indictment is based. See Record Documents 51-1 and 54.

However, Count 1 of the indictment charged Defendants with conspiracy to operate an unlicensed MSB under 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 1960 (unlicensed money transmitting businesses). Under 18 U.S.C. § 1960, a person commits an offense when he “knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business.” The statute defines the term “unlicensed money transmitting business” as “a money transmitting business which affects interstate or foreign commerce in any manner or degree” and either (A) is operated without an appropriate money transmitting license in a State; or (B) fails to comply with the money transmitting business registration requirements under 31 U.S.C. § 5330 or regulations thereunder. 18 U.S.C. § 1960(b)(1)(A) and (B). Thus, the statute sets forth two separate methods by which the Government may prove that a defendant is an “unlicensed money transmitting business”: failure to obtain a state license where such a license is necessary, or failure to comply with separate federal registration requirements.

Though the Government now concedes that it cannot prove the first method, the evidence the Government presented at the guilty plea hearing is nonetheless sufficient to prove the second method. Regulations promulgated under 31 U.S.C. § 5330 and other statutes define a “money service business” as a business engaging in at least one of several different varieties of financial business. 31 C.F.R. § 1010.100(ff). One such variety is a “money transmitter,” a person that engages in “the acceptance of currency, funds, or other value that substituted for currency from one person and the transmission

of currency, funds, or other value that substituted for currency to another location or person by any means.” 31 C.F.R. § 1010.100(ff)(5)(A). All businesses that meet the definition of “money services businesses” must register with FinCEN through the registration procedures set forth in 31 C.F.R. § 1022.380. One such requirement is that an MSB must submit its registration form to FinCEN within 180 days of the date the business is established. See 31 C.F.R. § 1022.380(b)(3).

As stated in the Factual and Procedural Background, *supra*, FinCEN released interpretive guidance in March 2013 clarifying the application of these regulations to businesses like that of Defendants. See Dept. of the Treasury, FinCEN, FIN-2013-G001, <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (March 18, 2013). This guidance clarified that though a user of a virtual currency like bitcoin is not an MSB, “an administrator or exchanger *is* an MSB under FinCEN’s regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person.” See id. at 1 (emphasis in original). It is undisputed that Defendants failed to register with FinCEN until November 2014, well past the 180-day deadline for such registration, which commenced sometime in 2013 when Defendants first began their bitcoin exchange business. See Record Document 42 at 11-25 (guilty plea testimony of Darrin Heusel, IRS Criminal Investigations Division). Thus, because “it is unlawful to do business [as an MSB] without complying with 31 U.S.C. § 5330 and [31 C.F.R. § 1022.380]” regardless of compliance with any state licensing requirements, the Court finds that Defendants have not asserted their actual innocence of the crime to which they pleaded guilty in Count 1 of the indictment. 31 C.F.R. § 1022.380(e).

Most of the other factors to consider in deciding a motion to withdraw a guilty plea also weigh in favor of denying the instant Motion. On the second factor, the Court finds that the Government would suffer some prejudice if the Motion were granted, as it would be required to prove the allegations in the indictment at trial.

On the third factor, the Court finds that the Defendants have delayed in filing the instant Motion to Withdraw their guilty plea. Defendants were aware that the State of Louisiana does not require a license for operating a bitcoin exchange business by August 2016. In a Sentencing Memorandum in August 2016, Defendants attached a letter determination from the Louisiana OFS to another bitcoin exchanger. See Record Document 43-2. That letter stated that such a business was not required to obtain a license from the State of Louisiana. See id. Thus, Defendants were aware that the State of Louisiana does not require such a license by August 2016 at the latest. In the instant Motion, Defendants assert that they have also recently contacted the OFS themselves to confirm this fact, and that the OFS confirmed that Louisiana does not require such a license. See Record Document 51-1 at 2-3. However, Defendants did not file the instant Motion until February 2017 when they knew that no state license was required by August 2016 at the latest. See Record Document 51. Thus, they waited almost six months after learning of the facts constituting the basis for the instant Motion before filing the Motion, a significant delay.

On the fourth factor, the Court finds that though withdrawing the guilty plea may not *substantially* inconvenience the Court, it would nonetheless require the Court to hold a multi-day trial on fifteen separate counts. Thus, granting the instant Motion would result in at least some inconvenience to the Court. On the fifth factor, the Court finds

that the assistance of counsel was available to Defendants throughout the instant action. Defendants were represented by extremely experienced criminal defense counsel from the first day of these proceedings, as their counsel enrolled in this case on the date of Defendants' initial appearance. See Record Document 16.

On the sixth factor, the Court finds that the plea to Count 1 was knowing and voluntary. At their guilty plea hearing, the Court questioned Defendants extensively, asking questions regarding their competence to enter a guilty plea, their waiver of significant constitutional rights, whether they were in fact guilty as charged, whether their decision to plead guilty was free and voluntary, and whether their decision to plead guilty was made with the advice and consent of their attorney. See Record Document 42 at 43-50. Nothing in Defendants' responses to these questions brought the voluntary nature of the guilty plea into question, challenged the ability of the Government to prove its case against Defendants, or indicated that Defendants had decided to plead guilty without the advice of counsel. See id. On the seventh factor, the Court finds that allowing Defendants to withdraw their guilty pleas would waste some judicial resources, such as the time expended on the guilty plea hearing. Thus, the Court finds that the factors it must consider in deciding whether Defendants have presented a "fair and just" reason to withdraw their guilty pleas to Count 1 weigh in favor of denying the instant Motion. Fed. R. Crim. P. 11(d)(2)(B).

B. Michael Lord May Not Withdraw His Guilty Plea to Count 15.

Defendants' Motion contains no arguments related to Michael Lord's guilty plea to Count 15 of the indictment, the count accusing him of participation in a drug conspiracy. See Record Document 51-1. Thus, it is unclear whether Michael Lord

actually seeks to withdraw his guilty plea as to Count 15, but because of the somewhat broad language used in the Motion itself, the Court will address Count 15 as well. See id. Michael Lord has presented no arguments that constitute a “fair and just” reason for withdrawing his guilty plea on this count, and does not claim innocence of that count. Fed. R. Crim. P. 11(d)(2)(B). The analysis of the other relevant factors is similar to the analysis of these factors for Count 1 in Section II, B, *supra*. Thus, Michael Lord may not withdraw his guilty plea on Count 15.

CONCLUSION

The ability to withdraw a guilty plea with approval of the Court is “not intended to allow a defendant to withdraw his guilty plea simply because he has changed his mind after further reflection.” United States v. Daniel, 866 F.2d 749, 751 (5th Cir. 1989). Defendants failed to provide a “fair and just” reason for the Court to permit withdrawal of their guilty pleas. Fed. R. Crim. P. 11(d)(2)(B). Most of the factors the Court must consider in deciding a motion to withdraw a guilty plea weigh in favor of denying the instant Motion. Therefore, Defendants’ Motion to Withdraw their guilty pleas (Record Document 51) is **DENIED**.

THUS DONE AND SIGNED at Shreveport, Louisiana, on this the 20th day of April, 2017.



S. MAURICE HICKS, JR.
UNITED STATES DISTRICT JUDGE

EXHIBIT

N

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
SHREVEPORT DIVISION

UNITED STATES OF AMERICA

CASE NO. 5:15-CR-00240-01-02

VERSUS

JUDGE HICKS

MICHAEL A. LORD (01)
RANDALL B. LORD (02)

MAGISTRATE JUDGE HORNSBY

MINUTES OF COURT:
Completion of Sentencing Hearing

| | | |
|-------------------|--------------|------------------------------------|
| Date: | May 24, 2017 | Presiding: Judge S. Maurice Hicks |
| Court Opened: | 9:30 A.M. | Courtroom Deputy: Denise McDonnell |
| Court Adjourned: | 5:10 P.M. | Court Reporter: Marie Moran Runyon |
| Statistical Time: | 05:00 | |

APPEARANCES

| | | |
|----------------------------|-----|--|
| Cytheria Jernigan (AUSA) | For | United States of America |
| Paul J. Carmouche (RET) | For | Defendants, Michael A. Lord and Randall B. Lord |
| Michael A. Lord, Defendant | | Defendant on bond |
| Randall B. Lord, Defendant | | Defendant on bond |

PROCEEDINGS

PROCEEDINGS:

Objections to PSR addressed and ruled on accordingly
Defendants advised of right to appeal

This matter was carried over from May 23, 2017. Testimony, evidence, and oral arguments were heard regarding Count 15 Drug Conspiracy as to Michael A. Lord (01).

Defendants' oral motion for forfeiture hearing was granted. The Government's memorandum regarding foreseeable issues is due within 14 days, and the Defendants' response is due 7 days from the Government's memorandum. The forfeiture matter is held open pending a hearing on June 5, 2017 at 10:00 a.m. or other resolution. The Court ordered that appellate delays shall not begin to run until after the forfeiture matter has been dealt with and a final judgment combining imprisonment plus forfeiture is entered in accordance with the law.

15-CR-240-01-02

May 24, 2017

Page Two

Michael A. Lord (01) is sentenced as follows:

The Court adopts the factual findings of the Probation Office as contained in the Presentencing Report, its addendum, and by oral rulings in open Court.

Pursuant to the Sentencing Reform Act of 1984 and in accordance with 18 U.S.C. §3553(a), the defendant is hereby committed to the custody of the Bureau of Prisons for a term of 46 months as to Count One of the Indictment and 60 months as to Count 15 of the Indictment, said terms to run consecutive with each other for a total term of imprisonment of 106 months. The defendant shall self-report to the institution designated by Federal Bureau of Prisons facility no later than 2:00 p.m. on July 11, 2017.

Upon release from confinement, the defendant shall be placed on supervised release for a term of 3 years as to each Count, to run concurrently.

The defendant was ordered to pay a \$200.00 special assessment to the Crime Victim Fund. No fine is ordered.

All remaining counts are hereby dismissed.

The defendant is notified of the right to appeal. If a notice of appeal is filed under 18 U.S.C. §3742, a Review of Sentence, the Clerk is directed to transmit the Presentence Report, under seal, to the Court of Appeals. If defendant wishes to appeal, Paul J. Carmouche shall file the Notice of Appeal. The Federal Public Defender's Office will be appointed to prosecute any Notice of Appeal.

Randall B. Lord (02) is sentenced as follows:

The Court adopts the factual findings of the Probation Office as contained in the Presentencing Report, its addendum, and by oral rulings in open Court.

Pursuant to the Sentencing Reform Act of 1984 and in accordance with 18 U.S.C. §3553(a), the defendant is hereby committed to the custody of the Bureau of Prisons for a term of 46 months as to Count One of the Indictment. The defendant shall self-report to the institution designated by the Federal Bureau of Prisons facility no later than 2:00 p.m. on July 11, 2017.

Upon release from confinement, the defendant shall be placed on supervised release for a term of 1 year.

15-CR-240-01-02

May 24, 2017

Page Three

The defendant was ordered to pay a \$100.00 special assessment to the Crime Victim Fund. No fine is ordered.

All remaining counts are hereby dismissed.

The defendant is notified of the right to appeal. If a notice of appeal is filed under 18 U.S.C. §3742, a Review of Sentence, the Clerk is directed to transmit the Presentence Report, under seal, to the Court of Appeals. If defendant wishes to appeal, Paul J. Carmouche shall file the Notice of Appeal. The Federal Public Defender's Office will be appointed to prosecute any Notice of Appeal.

EXHIBIT

O

Approved:


SERRIN TURNER

Assistant United States Attorney

ORIGINAL

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

UNITED STATES OF AMERICA

- v. -

ROBERT M. FAIELLA,
a/k/a "BTCKing," and
CHARLIE SHREM,

Defendants.

SEALED COMPLAINT

Violations of
18 U.S.C. §§ 1960 & 1956;
31 U.S.C. §§ 5318(g) &
5322(a)

COUNTY OF OFFENSE:
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 website¹, 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 "lbtck@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 than \$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 "l11a@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 "l11a 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 "l11a@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."

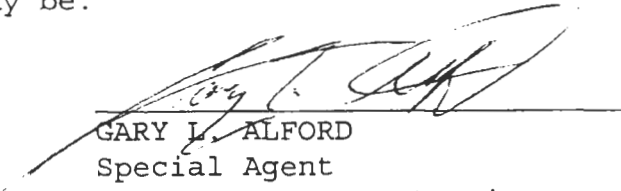
58. Similarly, as referenced in paragraph 43.c.iv, in an e-mail sent to SHREM, "BTCKing" mentioned he was "52 years old." This matches the age of ROBERT M. FAIELLA, the defendant.

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

EXHIBIT

P

AO 245B (Rev. 09/11) Judgment in a Criminal Case Sheet 1

UNITED STATES DISTRICT COURT

Southern District of New York

UNITED STATES OF AMERICA
v.
CHARLIE SHREM

JUDGMENT IN A CRIMINAL CASE

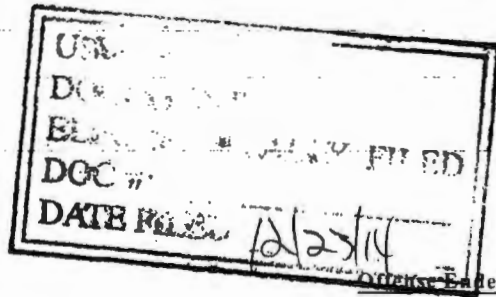
Case Number: S14CR243-02(JSR)

USM Number: 92164-054

Marc Agnifilo, Esq.
Defendant's Attorney

THE DEFENDANT:

- pleaded guilty to count(s) 1
pleaded nolo contendere to count(s) which was accepted by the court.
was found guilty on count(s) after a plea of not guilty.



The defendant is adjudicated guilty of these offenses:

Table with 4 columns: Title & Section, Nature of Offense, Date Filed, Count. Row 1: 18U.S.C.1960 &2, Aiding and Abetting the Operation of an Unlicensed Money Transmitting Business, 10/31/2012, 1

The defendant is sentenced as provided in pages 2 through 6 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

- The defendant has been found not guilty on count(s)
Count(s) is/are dismissed on the motion of the United States.
Underlying Indictment is/are dismissed on the motion of the United States.
Motion(s) is/are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid.

12/19/2014
Date of Imposition of Judgment

Signature of Judge (Handwritten signature)

Hon. Jed S. Rakoff, U.S.D.J.
Name and Title of Judge

Date 12/22/14

DEFENDANT: CHARLIE SHREM
CASE NUMBER: S14CR243-02(JSR)

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

On Count 1: Twenty four (24) months.

The court makes the following recommendations to the Bureau of Prisons:

Incarceration at Otisville.

The defendant is remanded to the custody of the United States Marshal.

The defendant shall surrender to the United States Marshal for this district:

at a.m. p.m. on

as notified by the United States Marshal.

The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

before 2 p.m. on 3/16/2015

as notified by the United States Marshal.

as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____

a _____, with a certified copy of this judgment.

UNITED STATES MARSHAL

By _____

DEPUTY UNITED STATES MARSHAL

DEFENDANT: CHARLIE SHREM
CASE NUMBER: S14CR243-02(JSR)

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of :

On Count 1: Three (3) years.

The defendant must report to the probation office in the district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

The defendant shall not commit another federal, state or local crime.

The defendant shall not unlawfully possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

- The above drug testing condition is suspended, based on the court's determination that the defendant poses a low risk of future substance abuse. *(Check, if applicable.)*
- The defendant shall not possess a firearm, ammunition, destructive device, or any other dangerous weapon. *(Check, if applicable.)*
- The defendant shall cooperate in the collection of DNA as directed by the probation officer. *(Check, if applicable.)*
- The defendant shall comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which he or she resides, works, is a student, or was convicted of a qualifying offense. *(Check, if applicable.)*
- The defendant shall participate in an approved program for domestic violence. *(Check, if applicable.)*

If this judgment imposes a fine or restitution, it is a condition of supervised release that the defendant pay in accordance with the Schedule of Payments sheet of this judgment.

The defendant must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached page.

STANDARD CONDITIONS OF SUPERVISION

- 1) the defendant shall not leave the judicial district without the permission of the court or probation officer;
- 2) the defendant shall report to the probation officer in a manner and frequency directed by the court or probation officer;
- 3) the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
- 4) the defendant shall support his or her dependents and meet other family responsibilities;
- 5) the defendant shall work regularly at a lawful occupation, unless excused by the probation officer for schooling, training, or other acceptable reasons;
- 6) the defendant shall notify the probation officer at least ten days prior to any change in residence or employment, or if such prior notification is not possible, then within five days after making such change.
- 7) the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician;
- 8) the defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered;
- 9) the defendant shall not associate with any persons engaged in criminal activity and shall not associate with any person convicted of a felony, unless granted permission to do so by the probation officer;
- 10) the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer;
- 11) the defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;
- 12) the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court; and
- 13) as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

AO 245B (Rev. 09/11) Judgment in a Criminal Case
Sheet 3C — Supervised Release

Judgment — Page 4 of 6

DEFENDANT: CHARLIE SHREM
CASE NUMBER: S14CR243-02(JSR)

SPECIAL CONDITIONS OF SUPERVISION

1. The Court recommends that the defendant be supervised by the district of residence.

DEFENDANT: CHARLIE SHREM
CASE NUMBER: S14CR243-02(JSR)

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

| | | | |
|---------------|-------------------|-------------|--------------------|
| | <u>Assessment</u> | <u>Fine</u> | <u>Restitution</u> |
| TOTALS | \$ 100.00 | \$ | \$ |

- The determination of restitution is deferred until . An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.
- The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

| | | | |
|----------------------|--------------------|----------------------------|-------------------------------|
| <u>Name of Payee</u> | <u>Total Loss*</u> | <u>Restitution Ordered</u> | <u>Priority or Percentage</u> |
|----------------------|--------------------|----------------------------|-------------------------------|

| | | |
|---------------|----|----|
| TOTALS | \$ | \$ |
|---------------|----|----|

- Restitution amount ordered pursuant to plea agreement \$
- The defendant must pay interest on restitution and a fine of more than \$2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).
- The court determined that the defendant does not have the ability to pay interest and it is ordered that:
 - the interest requirement is waived for the fine restitution.
 - the interest requirement for the fine restitution is modified as follows:

* Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: CHARLIE SHREM
CASE NUMBER: S14CR243-02(JSR)

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

- A Lump sum payment of \$ 100.00 due immediately, balance due
 - not later than _____, or
 - in accordance C, D, E, or F below; or
- B Payment to begin immediately (may be combined with C, D, or F below); or
- C Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after the date of this judgment; or
- D Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after release from imprisonment to a term of supervision; or
- E Payment during the term of supervised release will commence within _____ (e.g., 30 or 60 days) after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or
- F Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

Joint and Several

Defendant and Co-Defendant Names and Case Numbers (including defendant number), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

The defendant shall pay the cost of prosecution.

The defendant shall pay the following court cost(s):

The defendant shall forfeit the defendant's interest in the following property to the United States:
\$950,000 in US currency.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) penalties, and (8) costs, including cost of prosecution and court costs.

EXHIBIT

Q

AO 245B (Rev. 09/11) Judgment in a Criminal Case Sheet 1

UNITED STATES DISTRICT COURT

Southern District of New York

UNITED STATES OF AMERICA
v.
Robert Faiella

JUDGMENT IN A CRIMINAL CASE

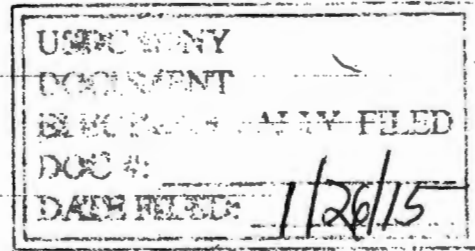
Case Number: 1: 14cr243-01(JSR)

USM Number: 09829-049

Timothy Treanor, Esq.
Defendant's Attorney

THE DEFENDANT:

- pleaded guilty to count(s) 1
pleaded nolo contendere to count(s) which was accepted by the court.
was found guilty on count(s) after a plea of not guilty.



The defendant is adjudicated guilty of these offenses:

Table with 4 columns: Title & Section, Nature of Offense, Offense Ended, Count. Row 1: 18U.S.C.1960(b)(1)(B), Operating an Unlicensed Money Transmitting Business, 10/13/2013, 1

The defendant is sentenced as provided in pages 2 through 6 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

- The defendant has been found not guilty on count(s)
Count(s) 2,3 and 4
Underlying
Motion(s)
is are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid.

1/20/2015
Date of Imposition of Judgment

Signature of Judge (Handwritten signature)

Hon. Jed S. Rakoff, U.S.D.J.
Name and Title of Judge

Date 1/20/15

AO 245B (Rev. 09/11) Judgment in Criminal Case
Sheet 2 — Imprisonment

Judgment — Page 2 of 6

DEFENDANT: Robert Faiella
CASE NUMBER: 1:14cr243-01(JSR)

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

ON COUNT 1: FORTY-EIGHT (48) MONTHS.

The court makes the following recommendations to the Bureau of Prisons:

Incarceration in a facility able to attend to the defendant's medical needs.

The defendant is remanded to the custody of the United States Marshal.

The defendant shall surrender to the United States Marshal for this district:

at a.m. p.m. on

as notified by the United States Marshal.

The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

before 2 p.m. on 3/3/2015

as notified by the United States Marshal.

as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____

a _____, with a certified copy of this judgment.

UNITED STATES MARSHAL

By

DEPUTY UNITED STATES MARSHAL

DEFENDANT: Robert Faiella
CASE NUMBER: 1: 14cr243-01(JSR)

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of :

On Count 1 : Three (3) years .

The defendant must report to the probation office in the district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

The defendant shall not commit another federal, state or local crime.

The defendant shall not unlawfully possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

- The above drug testing condition is suspended, based on the court's determination that the defendant poses a low risk of future substance abuse. *(Check, if applicable.)*
- The defendant shall not possess a firearm, ammunition, destructive device, or any other dangerous weapon. *(Check, if applicable.)*
- The defendant shall cooperate in the collection of DNA as directed by the probation officer. *(Check, if applicable.)*
- The defendant shall comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which he or she resides, works, is a student, or was convicted of a qualifying offense. *(Check, if applicable.)*
- The defendant shall participate in an approved program for domestic violence. *(Check, if applicable.)*

If this judgment imposes a fine or restitution, it is a condition of supervised release that the defendant pay in accordance with the Schedule of Payments sheet of this judgment.

The defendant must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached page.

STANDARD CONDITIONS OF SUPERVISION

- 1) the defendant shall not leave the judicial district without the permission of the court or probation officer;
- 2) the defendant shall report to the probation officer in a manner and frequency directed by the court or probation officer;
- 3) the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
- 4) the defendant shall support his or her dependents and meet other family responsibilities;
- 5) the defendant shall work regularly at a lawful occupation, unless excused by the probation officer for schooling, training, or other acceptable reasons;
- 6) the defendant shall notify the probation officer at least ten days prior to any change in residence or employment, or if such prior notification is not possible, then within five days after making such change.
- 7) the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician;
- 8) the defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered;
- 9) the defendant shall not associate with any persons engaged in criminal activity and shall not associate with any person convicted of a felony, unless granted permission to do so by the probation officer;
- 10) the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer;
- 11) the defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;
- 12) the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court; and
- 13) as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

AO 245B (Rev. 09/11) Judgment in a Criminal Case
Sheet JC — Supervised Release

Judgment—Page 4 of 6

DEFENDANT: Robert Faiella
CASE NUMBER: 1: 14cr243-01(JSR)

SPECIAL CONDITIONS OF SUPERVISION

1. The Court recommends that the defendant be supervised by the district of residence.

AO 245B (Rev. 09/11) Judgment in a Criminal Case
Sheet 5 - Criminal Monetary Penalties

Judgment -- Page 5 of 6

DEFENDANT: Robert Faiella
CASE NUMBER: 1:14cr243-01(JSR)

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

| | | | | | |
|--------|-------------------|--|-------------|--|--------------------|
| | <u>Assessment</u> | | <u>Fine</u> | | <u>Restitution</u> |
| TOTALS | \$ 100.00 | | \$ | | \$ |

- The determination of restitution is deferred until . An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.
- The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

| | | | |
|----------------------|--------------------|----------------------------|-------------------------------|
| <u>Name of Payee</u> | <u>Total Loss*</u> | <u>Restitution Ordered</u> | <u>Priority or Percentage</u> |
|----------------------|--------------------|----------------------------|-------------------------------|

| | | |
|--------|----|----|
| TOTALS | \$ | \$ |
|--------|----|----|

- Restitution amount ordered pursuant to plea agreement \$
- The defendant must pay interest on restitution and a fine of more than \$2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).
- The court determined that the defendant does not have the ability to pay interest and it is ordered that:
 - the interest requirement is waived for the fine restitution.
 - the interest requirement for the fine restitution is modified as follows:

* Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: Robert Faiella
CASE NUMBER: 1: 14cr243-01(JSR)

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

- A Lump sum payment of \$ **100.00** due immediately, balance due
 - not later than _____, or
 - in accordance C, D, E, or F below; or
- B Payment to begin immediately (may be combined with C, D, or F below); or
- C Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after the date of this judgment; or
- D Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after release from imprisonment to a term of supervision; or
- E Payment during the term of supervised release will commence within _____ (e.g., 30 or 60 days) after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or
- F Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

Joint and Several

Defendant and Co-Defendant Names and Case Numbers (including defendant number), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

The defendant shall pay the cost of prosecution.

The defendant shall pay the following court cost(s):

The defendant shall forfeit the defendant's interest in the following property to the United States:
\$950,000.00

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) penalties, and (8) costs, including cost of prosecution and court costs.

EXHIBIT

R

Philadelphia Inquirer: <http://www.philly.com/philly/business/bitcoin-crime-nets-pa-heroin-trafficker-prison-time-20180228.html>

Bitcoin crime nets prison time for Pa. heroin trafficker

Updated: February 28, 2018 — 6:17 PM EST

by Sam Wood, Staff Writer @samwoodiii | samwood@phillynews.com

A Pennsylvania man who illegally sold \$1.5 million in bitcoin to undercover federal agents and others was sentenced Wednesday to a year and a day in prison and will be required to surrender \$40,000 he made in commissions.

In one of the first cases of its kind, Eldon Stone Ross, 24, had been charged with conducting an unlicensed money transmitting business between January 2015 and November 2016 and failing to report the cash-to-bitcoin and bitcoin-to-cash transactions.

"We don't see many of these cases," said Bert Glenn, the assistant U.S. Attorney who prosecuted the case in Philadelphia. "It's the first I've done here."

Bitcoin is a virtual currency that has legitimate uses. However, due to the relative anonymity it provides users, it's often a preferred method of payment for illegal goods and services bought on the darkest corners of the Internet.

Commercial institutions such as Coinbase, which operate legal cryptocurrency exchanges, are required by federal law to report any suspicious transactions involving more than \$10,000 in cash to the Department of the Treasury as a safeguard against money laundering, extortion, and other illicit activities.

"If people can go to someone like Ross who is dealing outside the institutional market, it adds to their anonymity," Glenn said.

Ross admitted in October to selling \$50,000 worth of Bitcoin to undercover agents working with Homeland Security Investigations. In each case, he "failed to obtain identifying information from the agents," according to court records.

Ross, of Kennett Square, previously had been convicted in 2014 on felony charges of trafficking heroin and sentenced to up to 23 months in Chester County. He was apparently in jail during part of the period in which he admitted to operating the money transmitting business. According to court records, Ross petitioned to be released on house arrest in February 2015.

In addition to the year-long federal prison term, Ross will be required to serve three years of supervised release.