

FILED
2017 JAN 17 P 4:38
CLERK, U.S. DISTRICT COURT
NO. DIST. OF CA.

1 BRIAN J. STRETCH (CABN 163973)
United States Attorney

2 BARBARA J. VALLIERE (DCBN 439353)
3 Chief, Criminal Division

4 WIL FRENTZEN (LABN 24421)
Assistant United States Attorney
5 450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
6 Telephone: (415) 436-6959
7 Fax: (415) 436-7234
William.Frentzen@usdoj.gov

**SEALED
BY COURT ORDER**

8 Attorneys for the United States

9
10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12 SAN FRANCISCO DIVISION

13 UNITED STATES OF AMERICA,
14 Plaintiff,
15 v.
16 BTC-E, A/K/A CANTON BUSINESS
CORPORATION,
17 and
18 ALEXANDER VINNIK.
19 Defendants.
20

) CASE NO: CR 16-00227 SI
) UNITED STATES' MOTION TO SEAL
) SUPERSEDING INDICTMENT, ARREST
) WARRANTS AND ~~PROPOSED~~ ORDER

) UNDER SEAL

1 The United States hereby moves the Court for an order sealing this Motion and Order, Arrest
2 Warrants and the Superseding Indictment. The government believes that if the defendants are made
3 aware of these documents before they are arrested, that they may make efforts to avoid being arrested.

4
5
6 Date: January 17, 2017

Respectfully Submitted,

7 BRIAN J. STRETCH
8 United States Attorney

9
10 
11 WILLIAM FRENTZEN
12 Assistant United States Attorney

13 [Ⓢ]
14 **[PROPOSED] ORDER**

15 Based upon the foregoing request, the Court hereby **ORDERS** that this Motion and Order, Arrest
16 Warrants and the Superseding Indictment shall be filed and kept under seal by the clerk of the Court
17 until further order of the Court. The Court hereby further **ORDERS** that any representative of the
18 United States Attorney's Office or the Internal Revenue Service, shall be allowed to obtain a copy of the
19 Superseding Indictment without further order of the Court.

20
21 Dated: January 17, 2017

22 
23 HON. SALLIE KIM
24 UNITED STATES MAGISTRATE JUDGE

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

2017 JAN 17 P 4:38
SU... LUNG
CLERK, US DISTRICT COURT
NO. DIST. OF CA.

UNITED STATES OF AMERICA,

SEALED v.
BY COURT ORDER

CR 16-0227-SI

BTC-E, A/K/A CANTON BUSINESS CORPORATION
and ALEXANDER VINNIK,

DEFENDANT(S).

SUPERSEDING INDICTMENT

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;
18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;
18 U.S.C. § 1956(a)(1) - Money Laundering;
18 U.S.C. § 1957 - Unlawful Monetary Transactions; and
18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

A true bill.

[Signature]

Foreman

Filed in open court this 17th day of

January, 2017

[Signature]

Clerk

SALLIE KIM

United States Magistrate Judge

NO BAIL WARRANT
for Alexander Vinnik

Bail, \$

NO PROCESS *for BTC-E*

[Signature]

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: COMPLAINT INFORMATION INDICTMENT
 SUPERSEDING

OFFENSE CHARGED

- 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) - Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. § 982(a)(1) - Criminal Forfeiture
- Petty
 Minor
 Misdemeanor
 Felony

PENALTY: Please see attachment.

SEALED BY COURT ORDER

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

▶ BTC-E, A/K/A CANTON BUSINESS CORPORATION

DISTRICT COURT NUMBER

CR 16-00227 SI

FILED
 JAN 17 2017
 SUSAN Y. SOONG
 CLERK U.S. DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Internal Revenue Service

person is awaiting trial in another Federal or State Court, give name of court

this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of:

U.S. ATTORNEY DEFENSE } SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

IS NOT IN CUSTODY

Has not been arrested, pending outcome of proceeding.
 1) If not detained give date any prior summons was served on above charges

2) Is a Fugitive

3) Is on Bail or Release from (show District)

IS IN CUSTODY

4) On this charge

5) On another conviction } Federal State

6) Awaiting trial on other charges
 If answer to (6) is "Yes", show name of institution

Has detainer been filed? Yes No } If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... If Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

This report amends AO 257 previously submitted

Name and Office of Person Furnishing Information on this form BRIAN J. STRETCH
 U.S. Attorney Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) WILLIAM FRENTZEN

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

SUMMONS NO PROCESS* WARRANT

Bail Amount: _____

If Summons, complete following:

Arraignment Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET

BTC-E, A/K/A CANTON BUSINESS CORPORATION

COUNT ONE: (18 U.S.C. §1960 – Operation of an Unlicensed Money Service Business)
5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: COMPLAINT INFORMATION INDICTMENT
 SUPERSEDING

OFFENSE CHARGED

- 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) - Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture
- Petty
- Minor
- Misdemeanor
- Felony

PENALTY: Please see attachment.

SEALED BY COURT ORDER

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

DEFENDANT - U.S.

ALEXANDER VINNIK

DISTRICT COURT NUMBER
CR 16-00227 SI

FILED
JAN 17 2017
SUSAN Y. SOONG
CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Internal Revenue Service

person is awaiting trial in another Federal or State Court, give name of court

this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of:
 U.S. ATTORNEY DEFENSE

SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person Furnishing Information on this form BRIAN J. STRETCH

U.S. Attorney Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) WILLIAM FRENTZEN

IS NOT IN CUSTODY

- Has not been arrested, pending outcome this proceeding.
- 1) If not detained give date any prior summons was served on above charges
- 2) Is a Fugitive
- 3) Is on Bail or Release from (show District)

IS IN CUSTODY

- 4) On this charge
 - 5) On another conviction } Federal State
 - 6) Awaiting trial on other charges
- If answer to (6) is "Yes", show name of institution

Has detainer been filed? Yes No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... If Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

SUMMONS NO PROCESS* WARRANT

Bail Amount _____

If Summons, complete following:

Arraignment Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET

ALEXANDER VINNIK

COUNT ONE: (18 U.S.C. §1960 – Operation of an Unlicensed Money Service Business)
5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than \$500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a \$100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

FILED
2017 JUN 17 P 4:38
CLERK OF DISTRICT COURT
NO. DIST. OF CA.

1 BRIAN J. STRETCH (CABN 163973)
United States Attorney

6 SEALED
7 BY COURT ORDER

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA,
12 Plaintiff,

13 v.

14 BTC-E, A/K/A CANTON BUSINESS
CORPORATION,

15 and

16 ALEXANDER VINNIK.

17 Defendants.

) UNDER SEAL

) CASE NO. CR 16-00227 SI

) VIOLATIONS: 18 U.S.C. § 1960 – Operation of an
) Unlicensed Money Service Business; 18 U.S.C.
) § 1956(h) – Conspiracy to Commit Money
) Laundering; 18 U.S.C. § 1956(a)(1) – Money
) Laundering; 18 U.S.C. § 1957 – Unlawful Monetary
) Transactions; 18 U.S.C. § 982(a)(1) – Criminal
) Forfeiture

) SAN FRANCISCO VENUE

19 SUPERSEDING INDICTMENT

20 The Grand Jury charges:

21 INTRODUCTORY ALLEGATIONS

22 At all times relevant to this Indictment:

23 1. Since at least approximately 2011 through and including the present, both dates being
24 approximate and inclusive, the defendant BTC-e operated as one of the world's largest and most widely
25 used digital currency exchanges. Since its inception, BTC-e processed several billion dollars worth of
26 monetary exchanges. BTC-e was an exchange for cybercriminals worldwide, and one of the principal
27 entities used to launder and liquidate criminal proceeds from digital currencies, including Bitcoin, to fiat
28

1 currencies,¹ including U.S. dollars, Euros, and Rubles. At all relevant times, the defendant
2 ALEXANDER VINNIK, together with individuals known and unknown, directed and supervised BTC-
3 e's operations and finances.

4 2. BTC-e was an international money-laundering scheme that, by virtue of its business
5 model, catered to criminals – and to cybercriminals in particular. Through VINNIK's efforts, BTC-e
6 emerged as one of the principal means by which cyber criminals around the world laundered the
7 proceeds of their illicit activity. BTC-e facilitated crimes, including computer hacking and ransomware,
8 fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.

9
10 3. BTC-e lacked basic anti-money laundering controls and policies and, as such, was
11 attractive to those who desired to conceal criminal proceeds as it made it more difficult for law
12 enforcement to trace and attribute funds.

13
14 4. Since its founding, BTC-e received criminal proceeds of numerous computer intrusions
15 and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics
16 distribution rings. Among other things, BTC-e accounts received substantial proceeds from the hack of
17 the now-defunct Mt. Gox digital currency exchange and also received a substantial portion of the
18 criminal proceeds from one of the largest ransomware schemes, CryptoWall.

19 5. As described further below, the defendants and their co-conspirators, including those
20 known and unknown to the Grand Jury, intentionally created, structured, and operated BTC-e as a
21 criminal business venture, one designed to help criminals launder their proceeds and one they
22 themselves used to launder criminal proceeds. The defendants thus attracted and maintained a customer
23 base that was heavily reliant on criminals.

24
25 6. Despite doing substantial business in the United States, BTC-e was not registered as a
26

27 ¹ Fiat currency is simply a currency established by government regulation or law, e.g. U.S.
28 Dollars, Euros, Japanese Yen, British Pounds, Russian Rubles, Chinese RMB, etc.

1 money services business with the United States Department of the Treasury's Financial Crimes
2 Enforcement Network ("FinCEN"), as federal law requires. As described further below, BTC-e had no
3 meaningful anti-money laundering processes in place and lacked an effective anti-money laundering
4 program, as federal law also requires.

5
6 7. This was in contrast to other registered digital currency exchanges that, through their
7 anti-money laundering programs, strove to avoid having their platforms used for criminal activity. Most
8 of those exchanges described their operations down to listing the names, photos, and backgrounds of
9 their management, the location of their businesses, and their regulatory compliance policies.

10 8. BTC-e relied on the use of shell companies and affiliate entities that were similarly
11 unregistered with FinCEN and lacked basic anti-money laundering and "Know Your Customer"
12 policies. These entities catered to an online and worldwide customer base, and electronically "muled"
13 fiat currency in and out of BTC-e. BTC-e's own website stated it was located in Bulgaria, yet
14 simultaneously stated it was subject to the laws of Cyprus. Meanwhile, BTC-e's managing shell
15 company, CANTON BUSINESS CORPORATION, was based in the Seychelles but affiliated with a
16 Russian phone number, and its web domains were registered to shell companies in countries including
17 Singapore, the British Virgin Islands, France, and New Zealand.

18 BACKGROUND

19
20 9. Bitcoin is a form of decentralized, convertible digital currency that existed through the
21 use of an online, decentralized ledger system.² Bitcoin is just one of many forms of digital currency.
22 There are many others, including litecoin, ethers, worldcoin, and dogecoin. However, bitcoin has the
23 largest market capitalization of any present form of decentralized digital currency.

24 10. While bitcoin mainly exists as an Internet-based form of currency, it is possible to "print
25 out" the necessary information and exchange bitcoin via physical medium. The currency is not issued
26

27
28 ² Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to
use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and
"bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

1 by any government, bank, or company, but rather is generated and controlled through computer software
2 operating via a decentralized network. To acquire bitcoin, a typical user will purchase them from a
3 Bitcoin seller or "exchanger." It is also possible to "mine" bitcoin by verifying other users' transactions.
4 Bitcoin is just one form of digital currency, and there are a significant number of other varieties of
5 digital currency.

6 11. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its
7 value from government regulation or law), or other convertible digital currencies. When a user wishes
8 to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency,
9 often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding
10 quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will
11 then typically attempt to broker the purchase with another user of the exchange that is trying to sell
12 bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a
13 seller, then the transaction can be completed.

14 12. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user's bitcoin
15 address. The bitcoin address is somewhat analogous to a bank account number, and is comprised of a
16 case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can
17 then conduct transactions with other Bitcoin users, by transferring bitcoin to their bitcoin addresses, via
18 the Internet.

19 13. Little to no personally identifiable information about the payer or payee is transmitted in
20 a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public
21 key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address.
22 Only the bitcoin address of the receiving party and the sender's private key are needed to complete the
23 transaction. These two keys by themselves rarely reflect any identifying information.

24 14. All bitcoin transactions are recorded on what is known as the blockchain. This is
25 essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing,
26 and updates approximately six times per hour. The blockchain records every bitcoin address that has
27 ever received a bitcoin and maintains records of every transaction for each bitcoin address.

28 15. Digital currencies, including bitcoin, have many known legitimate uses. However, much

1 like cash, bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the
2 ease with which bitcoin can be used to move funds with high levels of anonymity. As is demonstrated
3 herein, however, in some circumstances bitcoin payments may be effectively traced by analyzing the
4 blockchain.

5 BTC-E OVERVIEW

6
7 16. BTC-e was founded in or about 2011. In the years it operated, BTC-e has served
8 approximately 700,000 users worldwide, including numerous customers in the United States and
9 customers in the Northern District of California. BTC-e touts itself as “a platform for individuals
10 interested in buying and selling bitcoin using an assortment of world currencies;” in other words, a
11 digital currency exchange.

12
13 17. Through the work of VINNIK and others known and unknown to the Grand Jury, BTC-e
14 became one of the primary ways by which cybercriminals around the world transferred, laundered, and
15 stored the criminal proceeds of their illegal activities. U.S. dollars and Russian rubles were the most
16 frequently exchanged fiat currencies on the platform, while Bitcoin and litecoin were the most widely
17 exchanged digital currencies.

18
19 18. Because such a significant portion of BTC-e’s business was derived from suspected
20 criminal activity and given its global reach, the scope of the defendants’ unlawful conduct was massive.
21 During the relevant timeframe from 2011 to December 30, 2016, bitcoin addresses associated with BTC-
22 e had received over 9.4 million bitcoin. Bitcoin’s rapidly fluctuating exchange rate makes it difficult to
23 determine the U.S. Dollar value of this quantity of bitcoin over time. However, using today’s bitcoin
24 exchange rate, the total value of bitcoin received by BTC-e over the course of its operation would be
25 valued at over \$9 billion. In 2016 alone, BTC-e received over 1.8 million bitcoin, valued at over \$1.7
26 billion at today’s exchange rate.³

27
28 ³ This is calculated using the December 30, 2016 bitcoin trading value of approximately \$962 per
bitcoin. Since August 2011, the Bitcoin market price has fluctuated from a low of roughly \$2 to a high

1 19. Notably, the above figures only include bitcoin exchanged on the BTC-e platform and do
2 not even include the deposits and withdrawals made in other digital currencies, such as litecoin, nor do
3 these figures take into account well over a billion dollars' worth of what is known as "BTC-e code."
4 BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other
5 BTC-e users.
6

7 20. BTC-e maintained its servers in the United States. The servers were one of the primary
8 ways in which BTC-e and the defendants effectuated their operations. BTC-e also used many third-
9 party companies, including companies within the Northern District of California, to effectuate their
10 operations and enable them to function.

11 21. At its inception, BTC-e was one of a number of digital currency exchanges. It was
12 engaged in the same line of business as other online digital currency exchanges in existence at the time,
13 including Liberty Reserve. Liberty Reserve was a Costa Rica-based centralized digital currency service
14 that laundered approximately \$6 billion in criminal proceeds. It was shuttered in 2013 when its founder
15 and six other individuals were charged with conspiracy to commit money laundering and with operating
16 an unlicensed money transmitting business. Liberty Reserve's website was seized by the U.S.
17 government.⁴
18

19 22. There was an overlap between many Liberty Reserve users and BTC-e users. BTC-e
20 itself was a user of Liberty Reserve.
21

22 23. Another digital currency exchange in operation between 2011 and 2014 was the MTGOX
23 Exchange ("Mt. Gox") that was originally founded in San Francisco, but ultimately based in Tokyo,
24 Japan. In 2014, Mt. Gox collapsed, having been the target of a series of major intrusions that resulted in
25 thefts totaling several hundred million dollars worth of bitcoin. In 2014, Mt. Gox filed for bankruptcy in
26

27 of approximately \$1200 per bitcoin and has varied dramatically over time..
28

1 front for BTC-e's operations. Like BTC-e, CANTON was not registered with FinCEN. Financial and
2 other records demonstrate that CANTON was synonymous with BTC-e. VINNIK, a Russian national,
3 was a primary beneficial owner of CANTON's financial accounts. Although CANTON's listed
4 business address was in the Seychelles, it operated using a Russian telephone number.

5
6 30. VINNIK also operated and controlled multiple BTC-e accounts, including a BTC-e
7 account known as the "WME" account. The "WME" account was tied directly to BTC-e administrator
8 accounts. Numerous withdrawals from BTC-e administrator accounts went directly to bank accounts
9 tied to VINNIK.

10 31. Another such administrator account associated with VINNIK was the "Vammedam"⁵
11 account. The "Vammedam" account was directly linked to the BTC-e administrative, financial,
12 operational and support accounts, accounts to which only those involved in the operations of the BTC-e
13 enterprise would have had access. Proceeds from well-known hacks and thefts from bitcoin exchanges
14 and users around the world funded the Vammedam account. Out of the Vammedam account, large
15 payments were made to accounts associated with VINNIK and others known and unknown to the Grand
16 Jury, including a Russian national hereafter referred to as unindicted CO-CONSPIRATOR X, who is
17 alleged to have access to the Vammedam account.
18



19 BTC-E FUNCTION

20 32. To use BTC-e, one created an account by accessing the BTC-e website. A user did not
21 need to provide even the most basic identifying information such as name, date of birth, address, or
22 other identifiers. All that BTC-e required was a username, password, and an email address. Unlike
23 legitimate payment processors or digital currency exchangers, BTC-e did not require its users to validate
24 their identity information by providing official identification documents, given that BTC-e did not
25 require an identity at all.
26
27

28 ⁵ Vammedam means "I will not give it to you" in Russian.

1 33. Thus, a user could create a BTC-e account with nothing more than a username and email
2 address, which often bore no relationship to the identity of the actual user. Accounts were therefore
3 easily opened anonymously, including by customers in the United States within the Northern District of
4 California.

5 34. At all times relevant to this Indictment, BTC-e had no anti-money laundering and/or
6 "Know-Your-Customer" (KYC) processes and policies in place. As discussed above, BTC-e collected
7 virtually no customer data at all. Nor did BTC-e or its shell companies ever register with FinCEN or
8 perform these functions on BTC-e's behalf.

10 35. A user could fund a BTC-e account in numerous different ways. One way involved
11 funding the account with fiat currency that would be converted into digital currency, such as bitcoin.
12 With fiat currency, a user could initiate a wire transfer from a financial institution made directly for the
13 benefit of BTC-e to an account at another financial institution, which was routed to a bank account
14 maintained by one of BTC-e's shell or affiliated companies. 
15 

16
17
18
19
20
21 36. Another way involved funding a BTC-e account with a user's existing digital currency.
22 A user with existing digital currency, such as bitcoin, could fund a BTC-e account directly via bitcoin
23 deposits. BTC-e users could also purchase "BTC-e code" that could be sent and exchanged amongst
24 BTC-e users. BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital
25 currencies to other BTC-e users. This served as another conduit for money laundering as it allowed
26 BTC-e customers to withdraw funds from their BTC-e account and transfer them to other BTC-e users
27
28

1 anonymously.

2 37. BTC-e's business model obscured and anonymized transactions and source of funds. For
3 example, a BTC-e user could not fund an account by directly transferring money to BTC-e itself, but
4 rather had to wire funds to one of BTC-e's shells or affiliate entities. Nor could BTC-e users withdraw
5 funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were
6 required to make any deposits or withdrawals through the use of third-party "exchangers," thus enabling
7 BTC-e to avoid collecting any information about its users through banking transactions or other activity
8 that would leave a centralized financial paper trail.

10 38. Once a user funded an account with BTC-e, the user could then do any number of things:
11 conduct transactions with other BTC-e users; exchange digital currency into fiat currency; or simply use
12 BTC-e to store digital currency deposits, much like a bank.

13 39. Like other digital currency exchanges, BTC-e charged transaction fees for their services.
14 BTC-e charged a percentage fee every time a user transferred funds held in BTC-e to another user
15 through the BTC-e system. In addition, BTC-e charged a percentage fee every time a user used BTC-e
16 to exchange digital currency held in a BTC-e account into fiat currency.⁶

18 40. In addition to the fees BTC-e charged, users were charged additional fees by [REDACTED]
19 [REDACTED] each taking a percentage of the funds exchanged. These added fees were
20 associated with getting money in and out of the BTC-e platform through these funding mechanisms,
21 mechanisms that obfuscated the true sender of the currency.

22 41. Those engaged in criminal activity using BTC-e gravitated to BTC-e because of the site's
23 lack of anti-money laundering and "Know-Your-Customer" processes in place that could have them
24 reported to the government. Criminals who used BTC-e to launder funds were also willing to go to the
25 extra trouble of wiring money offshore to entities that operated through shell companies.
26

1 transfer funds among criminal associates. In particular, it was used by hacking and computer intrusion
2 rings operating around the world to distribute criminal proceeds of their endeavors. It was also used by
3 rings of identity thieves, corrupt public officials, narcotics distribution networks, and other criminals.

4 48. In fact, some of the largest known purveyors of ransomware used BTC-e as a means of
5 storing, distributing, and laundering their criminal proceeds. Ransomware is a criminal scheme in which
6 cybercriminals orchestrate the unwanted malicious download of encryption software on an unsuspecting
7 victim computer. It works as follows: once a victim is infected with the malicious software, often by
8 clicking on a fraudulent email, the ransomware will encrypt multiple files types on victim machines and
9 hold those files for ransom, requiring the victim to pay the administrators of the ransomware scheme in
10 order to have their files decrypted. Victims that pay the ransom are able to decrypt their files by using a
11 stand-alone program provided by the ransomware administrators after the ransom payment has been
12 made. The method of encryption implemented by the ransomware, if properly executed, renders it
13 impossible for victims to decrypt their encrypted files in any other way. The most prevalent payment
14 method accepted by current purveyors of ransomware is bitcoin.

15 49. One such ransomware scheme, CryptoWall, was distributed by methods including
16 fraudulent and phishing emails. CryptoWall was one of the most infamous varieties of ransomware and
17 has infected a vast number of computers across the world. During the timeframe relevant to this
18 Indictment, the purveyors of CryptoWall deposited and laundered many hundreds of thousands of
19 dollars' worth of ransom payments into BTC-e.

20 50. So, too, did a pair of corrupt U.S. federal agents, Carl Mark Force and Shaun Bridges, use
21 BTC-e to launder their criminal proceeds. Their experience with the criminal underworld taught them
22 that using BTC-e, as opposed to a registered exchange with anti-money laundering policies, would
23 maximize their chances of being able to conceal criminal proceeds. Each therefore sent several hundred
24 thousand dollars in criminal proceeds – derived from crimes ranging from theft of government property
25
26
27
28

1 to extortion – to the BTC-e platform for laundering.

2 51. BTC-e also served as the receptacle and transmitter of criminal funds from a series of
3 well-publicized computer intrusions and resulting thefts, including the well-publicized thefts from the
4 Japan-based Mt. Gox exchange. As discussed below, a sizable portion of the stolen Mt. Gox funds were
5 deposited into accounts controlled, owned, and operated by BTC-e and by defendant VINNIK and
6 others known and unknown to the Grand Jury.
7

8 52. The Mt. Gox exchange was the subject of a series of computer intrusions and resulting
9 thefts between approximately September 2011 and May 2014, in violation of Title 18, United States
10 Code, Section 1030(a)(4). Several hundred millions dollars' worth of bitcoin was stolen, including from
11 numerous customers in the U.S. and within the Northern District of California. After the thefts, some
12 approximately 530,000 of the bitcoin (worth hundreds of millions of dollars) stolen from Mt. Gox was
13 deposited into wallets at three different digital currency exchanges: (i) BTC-e; (ii) Trade Hill, another
14 exchange based in San Francisco; and (iii) back into Mt. Gox into a different Mt. Gox wallet.
15

16 53. Of this 530,000 bitcoin,⁷ 300,000 of it was sent directly to three separate BTC-e
17 accounts: "Vammedam," "Grmbit," and "Petr." These accounts were all linked to each other.
18

19 54. Meanwhile, blockchain analysis reveals that the stolen Mt. Gox funds that went to Trade
20 Hill and back into the other Mt. Gox account were controlled by a user who also controlled a BTC-e
21 account called "WME." At all times relevant to this Indictment, defendant VINNIK exercised control
22 over the BTC-e "WME" account.

23 55. The "Vammedam," "Grmbit," "Petr," and "WME" accounts were each directly linked to a
24 variety of different BTC-e administrative accounts, accounts for which only BTC-e administrators
25 and/or operators would have had access. The "Vammedam" account was similarly a
26
27

28 ⁷ The amount of bitcoin stolen from Mt. Gox accounted for just under half of the total thefts that Mt. Gox suffered.

1 56. VINNIK, along with others known and unknown, controlled and operated the
2 “Vannedam” account. Between approximately August 2013 and November 2015, CO-
3 CONSPIRATOR X and identities linked to VINNIK and to BTC-e received direct payments from the
4 “Vannedam” account to their own personal digital currency accounts at another digital currency
5 exchange, Bitstamp. These bitcoin were then exchanged into fiat currency and sent to bank accounts in
6 Cyprus and Latvia tied to VINNIK and other identities associated with VINNIK and BTC-e.
7

8 STATUTORY ALLEGATIONS

9 COUNT ONE: (18 U.S.C. § 1960 – Operation of an Unlicensed Money Transmitting Business)

10 57. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein
11 as if set forth in full.

12 58. Title 18, United States Code, Section 1960, makes it a crime to operate an unlicensed
13 money transmitting business. The term money transmitting includes “transferring funds on behalf of the
14 public by any and all means including but not limited to transfers within this country or to locations
15 abroad by wire, check, draft, facsimile, or courier.” This statute makes it a violation to conduct a
16 “money transmitting business” if the business is not registered as a money transmitting business with the
17 Secretary of the Treasury as required by a separate statute, Title 31, United States Code, Section 5330
18 and federal regulations pursuant to that statute.

19 59. The regulations specifically apply to foreign-based money transmitting businesses doing
20 substantial business in the United States. See C.F.R. §§ 1010.100(ff)(5), 1022.380(a)(2).

21 60. From in or about 2011, up to and including in or about May 2016, both dates being
22 approximate and inclusive, in the Northern District of California and elsewhere, the defendants,
23

24 BTC-e a/k/a CANTON BUSINESS CORPORATION, and
25 ALEXANDER VINNIK,

26 and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed,
27 supervised, directed, and owned all and part of a money transmitting business affecting interstate and
28 foreign commerce, i.e. BTC-e, which (i) failed to comply with the money transmitting business

1 registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations
2 prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5) and 1022.380(a)(2);
3 and (ii) otherwise involved the transportation and transmission of funds known to the defendants to have
4 been derived from a criminal offense and intended to be used to promote and support unlawful activity.

5 All in violation of Title 18, United States Code, Sections 1960 & 2.

6
7 COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

8 61. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein
9 as if set forth in full.

10 62. From in or about July 2011, through in or about January 2017, both dates being
11 approximate and inclusive, within the Northern District of California, and elsewhere, the defendants;

12 BTC-e a/k/a CANTON BUSINESS CORPORATION, and
13 ALEXANDER VINNIK,

14
15 and others known and unknown to the Grand Jury, willfully and knowingly did combine, conspire,
16 confederate, and agree together and with each other to knowingly conduct and attempt to conduct
17 financial transactions affecting interstate commerce and foreign commerce, which transactions involved
18 the proceeds of specified unlawful activity, that is, operation of an unregistered money transmitting
19 business in violation of Title 18, United States Code, Sections 1960; computer hacking and intrusions in
20 violation of Title 18, United States Code, Section 1030; identity theft in violation of Title 18, United
21 States Code, Section 1028; interstate transportation of stolen property in violation of Title 18, United
22 States Code, Section 2314; theft of government proceeds and extortion in violation of Title 18, United
23 States Code, Sections 641 and 1951; and narcotics trafficking in violation of Title 21, United States
24 Code, Section 841; with the intent to promote the carrying on of the specified unlawful activity, and that
25 while conducting and attempting to conduct such financial transactions, knew that the property involved
26 in the financial transactions represented the proceeds of some form of unlawful activity, in violation of
27 Title 18, United States Code, Section 1956(a)(1)(A)(i).

28 All in violation of Title 18, United States Code, Section 1956(h).

1 COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) – Money
2 Laundering)

3 On or about the dates described below, in the Northern District of California and elsewhere, the
4 defendant,

5 ALEXANDER VINNIK,

6 aided and abetted by others, known and unknown to the Grand Jury, did knowingly conduct and attempt
7 to conduct the listed financial transactions affecting interstate and foreign commerce which involved the
8 proceeds of a specified unlawful activity, that is accessing a computer in furtherance of fraud, in
9 violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A), with the intent to promote
10 the carrying on of said specified unlawful activity, and knowing that the transaction was designed in
11 whole and in part to conceal and disguise the nature, location, source, ownership, and proceeds of said
12 specified unlawful activity, and that while conducting and attempting to conduct such financial
13 transaction, knew that the property involved in the financial transaction represented the proceeds of
14 some form of unlawful activity.
15

16

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
THREE	01/23/2012	90 BTC	\$567.00	Transfer of BTC into Tradehill
FOUR	01/23/2012	83 BTC	\$522.07	Transfer of BTC into Tradehill
FIVE	01/23/2012	61 BTC	\$383.69	Transfer of BTC into Tradehill
SIX	01/24/2012	91 BTC	\$573.30	Transfer of BTC into Tradehill
SEVEN	01/24/2012	90 BTC	\$567.00	Transfer of BTC into Tradehill
EIGHT	01/24/2012	99 BTC	\$623.70	Transfer of BTC into Tradehill
NINE	01/24/2012	533 BTC	\$3,357.90	Transfer of BTC into Tradehill
TEN	01/24/2012	1900 BTC	\$11,970.00	Transfer of BTC into Tradehill
ELEVEN	01/24/2012	579 BTC	\$3,647.70	Transfer of BTC into Tradehill
TWELVE	01/24/2012	2 BTC	\$12.60	Transfer of BTC into Tradehill
THIRTEEN	01/27/2012	1000 BTC	\$5,290.00	Transfer of BTC into Tradehill
FOURTEEN	01/27/2012	1500 BTC	\$7,935.00	Transfer of BTC into Tradehill
FIFTEEN	02/01/2012	1000 BTC	\$5,820.00	Transfer of BTC into Tradehill
SIXTEEN	02/01/2012	1000 BTC	\$5,820.00	Transfer of BTC into Tradehill
SEVENTEEN	02/05/2012	3000 BTC	\$17,040.00	Transfer of BTC into Tradehill
EIGHTEEN	02/05/2012	500 BTC	\$2,840.00	Transfer of BTC into Tradehill
NINETEEN	02/12/2012	2000 BTC	\$11,200.00	Transfer of BTC into Tradehill

17
18
19
20
21
22
23
24
25
26

27 All in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i), (a)(1)(B)(i), and 2.
28

1
2
3 COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful
4 Monetary Transactions)

5 On or about the dates described below, in the Northern District of California and elsewhere, the
6 defendant,

7 ALEXANDER VINNIK,

8 aided and abetted by others, known and unknown to the Grand Jury, did knowingly engage and attempt
9 to engage in the listed monetary transactions by through or to a financial institution affecting interstate
10 and foreign commerce in criminally derived property of a value greater than \$10,000, that is the
11 transactions listed below, such property having been derived from a specified unlawful activity, that is
12 accessing a computer in furtherance of fraud, in violation of Title 18, United States Code, Section
13 1030(a)(4) and (c)(3)(A).

14

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
TWENTY	02/05/2012	3000 BTC	\$17,040.00	Transfer of BTC into Tradehill
TWENTY-ONE	02/12/2012	2000 BTC	\$11,200.00	Transfer of BTC into Tradehill

17 All in violation of Title 18, United States Code, Sections 1957 and 2.

18
19 FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

20 63. All of the allegations contained in this Indictment are re-alleged and by this reference
21 fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18,
22 United States Code, Section 982(a)(1).

23 64. Upon a conviction for any of the offenses alleged in this Indictment, the defendants,
24 BTC-e a/k/a CANTON BUSINESS CORPORATION, and
25 ALEXANDER VINNIK,
26 shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal,
27 involved in those offenses or any property traceable to such offenses including but not limited to a
28 forfeiture money judgment.

1 If any of the aforementioned property, as a result of any act or omission of the defendants

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

8 any and all interest the defendant has in other property shall be vested in the United States and

9 forfeited to the United States pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1).

10 All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal

11 Rules of Criminal Procedure.

12

13 DATED: 1/17/17

A TRUE BILL


14

15 
FOREPERSON


16

17 BRIAN J. STRETCH
United States Attorney

18

19 
20
21 BARBARA J. VALLIERE
Chief, Criminal Division

22

23 (Approved as to form: 
24 WILLIAM FRENTZEN
KATHRYN HAUN
25 Assistant U.S. Attorneys

**SEALED
BY COURT ORDER**

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

CRIMINAL COVER SHEET

Instructions: Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.

CASE NAME: BTC-E a/k/a Canton Business Corporation **CASE NUMBER:**
USA v. and Alexander Vinnik CR 16-00227 SI

Is This Case Under Seal? Yes No

Total Number of Defendants: 1 2-7 8 or more

Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326? Yes No

Venue (Per Crim. L.R. 18-1): SF OAK SJ

Is this a potential high-cost case? Yes No

Is any defendant charged with a death-penalty-eligible crime? Yes No

Is this a RICO Act gang case? Yes No

**Assigned AUSA
(Lead Attorney):** William Frentzen

Date Submitted: 01/17/2017

Comments:

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY



IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
SERVERS CONTAINING BTC-E-
RELATED CONTENT STORED AT THE
PREMISES CONTROLLED BY
EQUINIX

Mag. No. 17-8128

Leda Dunn Wettre

SEALING ORDER

This matter having been brought before the Court upon application of William E. Fitzpatrick, Acting United States Attorney for the District of New Jersey (Jason S. Gould, Assistant United States Attorney, appearing), for an order sealing the search warrant issued on this date and the application and attached Affidavit in support of that warrant, and for good cause shown,

IT IS on this 21st Day of July 2017,

ORDERED that the search warrant, the application and affidavit in support of the search warrant, and all related documents, except for one copy of the search warrant and inventory to be served at the time the search is executed, be and hereby are sealed until further Order of this Court.

Hon. Leda Dunn Wettre
United States Magistrate Judge



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu