1 DAVID L. ANDERSON (CABN 149604)
   United States Attorney
2
   SARA WINSLOW (DCBN 457643)
3 Chief, Civil Division

4 KIRSTIN M. AULT (CABN 206052)
   Assistant United States Attorney
5
        450 Golden Gate Avenue, Box 36055
6   San Francisco, California 94102-3495
        Telephone: (415) 436-6940
7   FAX: (415) 436-7234
        Kirstin.ault@usdoj.gov
8
   Attorneys for United States of America
9
                    UNITED STATES DISTRICT COURT
10
                 NORTHERN DISTRICT OF CALIFORNIA
11
                      SAN FRANCISCO DIVISION
12

13 UNITED STATES OF AMERICA,   ) CASE NO.
)
14   Plaintiff,   )
) **COMPLAINT**
15   v.   )
)
16 BTC-e, a/k/a CANTON BUSINESS CORP.,   )
)
17 and   )
)
18 ALEXANDER VINNIK,   )
)
19   Defendants.   )
)

20

21

22

23

24

25

26

27

28

COMPLAINT

1 The United States of America alleges as follows:

2 ### I. NATURE OF ACTION

3   1.   The United States brings this action against BTC-e a/k/a Canton Business Corporation

4 ("BTC-e") and Alexander Vinnik ("Vinnik") (collectively "Defendants"), to recover civil money

5 penalties imposed under the Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C.

6 §§ 5311-5314 and 5316-5332, which is commonly referred to as the Bank Secrecy Act ("BSA").

7 ### II. JURISDICTION AND VENUE

8   2.   This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C.

9 §§ 1331 and 1345. The Court may exercise personal jurisdiction over Defendants because they transact

10 business in this District.

11   3.   Venue is proper in the Northern District of California under 28 U.S.C. §§ 1391(b) and (c)

12 because Defendants transact business in this District.

13 ### III. PARTIES

14   4.   The United States brings this action on behalf of the Department of the Treasury.

15   5.   Defendant BTC-e is a corporation organized under the laws of either Cyprus and/or the

16 Seychelles Islands. BTC-e operated in Bulgaria, the Seychelles Islands, and other jurisdictions,

17 including the Northern District of California. At all times relevant to this complaint, BTC-e was a

18 money services business providing services subject to the BSA in the Northern District of California and

19 elsewhere.

20   6.   Defendant Alexander Vinnik is a Russian national who is currently incarcerated in

21 Greece. At all times relevant to this complaint, Vinnik occupied a senior leadership position within

22 BTC-e.

23 ### IV. THE BANK SECRECY ACT

24   7.   The Financial Crimes Enforcement Network ("FinCEN"), a bureau within the United

25 States Department of the Treasury, administers the BSA pursuant to authority delegated by the Secretary

26 of the Treasury. *See* Treasury Order 180-01 (July 1, 2014). The BSA requires the filing of reports and

27 the maintenance of records useful in criminal, tax, or regulatory investigations or proceedings, or in the

28 conduct of intelligence or counterintelligence activities to protect against international terrorism.

COMPLAINT   1

1   Regulations implementing the BSA appear at 31 C.F.R. Chapter X. Rules issued under the BSA require

2   the registration of money services businesses ("MSBs"), the filing of Suspicious Activity Reports

3   ("SARs"), the implementation of anti-money laundering ("AML") programs, and the maintenance of

4   records related to transmittals of funds.

5   8.   FinCEN may impose a civil monetary penalty "at any time before the end of the 6-year

6   period beginning on the date of the transaction with respect to which the penalty was assessed," and may

7   commence an action to recover the civil money penalty at any time before the end of the 2-year period

8   beginning on the date the penalty was imposed. *See* 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

9   9.   MSBs are "financial institutions" for purposes of the BSA and its implementing

10 regulations. *See* 31 U.S.C. § 5312(a)(2)(J), (K) and (R); 31 C.F.R. § 1010.100(t)(3). A "money services

11 business" is defined in regulations implementing the BSA to include persons who are engaged as a

12 business in providing money transmission services "wholly or in substantial part within the United

13 States." *See* 31 C.F.R. § 1010.100(ff)(5). Exchangers of convertible virtual currency provide "money

14 transmission services" for purposes of regulations implementing the BSA and may therefore qualify as

15 MSBs. *See* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering,

16 Exchanging, or Using Virtual Currencies" (March 18, 2013).

17   10.   FinCEN may impose on any person who owns or controls an unregistered MSB a civil

18 money penalty for each day that the MSB remains unregistered. *See* 31 U.S.C. § 5330(e)(2); 31 C.F.R.

19 § 1022.380(e). For MSB registration violations occurring on or before November 2, 2015, FinCEN may

20 assess a penalty of up to $7,954 for each violation. 31 C.F.R. § 1010.821. Violations occurring after

21 November 2, 2015, may be assessed in an amount up to $8,084 for each violation. *Id.* Each day a

22 violation continues constitutes a separate violation. 31 C.F.R. § 1022.380(e).

23   11.   FinCEN may impose a civil money penalty on a domestic financial institution that

24 willfully violates the BSA by failing to establish or maintain an adequate AML program and for failing

25 to file SARs as appropriate, and on any partner, director, officer or employee who willfully participates

26 in the violation. *See* 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820. The term "domestic" refers to "the

27 doing of business within the United States" or the performance of functions within the United States. 31

28 C.F.R. § 1010.100(o); *see also* 31 U.S.C. § 5312(b)(1). For violations occurring on or before November

2, 2015, FinCEN may impose a penalty of $25,000 to $100,000 for willful violations of BSA program requirements. 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f). For AML program violations after November 2, 2015, FinCEN may impose a penalty of $54,789 to $219,156. 31 C.F.R. § 1010.821. For violations of the requirement to implement an adequate AML program, "a separate violation occurs for each day that the violation continues." *See* 31 U.S.C. § 5321(a)(1) and 31 C.F.R. §1010.821.

V.   FACTUAL ALLEGATIONS

A.   Bitcoin and Digital Currencies

12.   Bitcoin is a form of decentralized, convertible digital currency that exists through the use of an online, decentralized ledger system. Bitcoin is just one of many forms of digital currency. There are many others, including litecoin, ether, worldcoin, and dogecoin; however, bitcoin has the largest market capitalization of any present form of decentralized digital currency. While bitcoin is an internet-based form of currency, it is possible to "print out" the necessary bitcoin information and exchange it via physical media. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire bitcoin, a typical user will purchase it from a bitcoin seller or "exchanger."

13.   Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value from government regulation or law), or other convertible digital currencies. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or automated clearing house ("ACH") transfer, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will then attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself.

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

15.   Little to no personally identifiable information about the payer or payee is transmitted in

COMPLAINT   3

1   a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public

2   key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address.

3   Only the bitcoin address of the receiving party and the sender's private key are needed to complete the

4   transaction. These two keys by themselves rarely reflect any information identifying the payer or payee.

5   16.   All bitcoin transactions are recorded on what is known as the Blockchain. The

6   Blockchain is a distributed public ledger that maintains all bitcoin transactions, incoming and outgoing.

7   The Blockchain records every bitcoin address that has ever received a bitcoin and maintains records of

8   every transaction for each bitcoin address. In some circumstances, bitcoin payments may be effectively

9   traced by analyzing the Blockchain.

10 **B.   BTC-e Operations**

11   17.   BTC-e was a digital currency exchange that allowed users to buy and sell bitcoin, and

12 other digital currencies, anonymously through its web domain btc-e.com. Since its founding, BTC-e has

13 served approximately 700,000 users worldwide, including numerous customers in the United States and

14 in the Northern District of California. BTC-e was used by cybercriminals worldwide and was one of the

15 principal entities used to launder and liquidate criminal proceeds, converting them from digital

16 currencies, including bitcoin, to fiat currencies, including U.S. Dollars, Euros, and Rubles.

17   18.   To use BTC-e, a user created an account by accessing BTC-e's website, www.btc-e.com.

18 To create an account, a user did not need to provide even the most basic identifying information, such as

19 name, date of birth, address, or other identifiers. All BTC-e required to create a user account was a self-

20 created username, password, and an email address. Unlike legitimate digital currency exchangers, BTC-

21 e did not require its users to validate their identity by providing official identification documents. When

22 a customer attempted to use bank wires to transfer funds to or from BTC-e's exchange, BTC-e at times

23 did request identifying documentation, such as a driver's license or passport. BTC-e did not request

24 such documents for all transactions involving bank wires or for other types of transactions.

25   19.   BTC-e's business model obscured and anonymized transactions and sources of funds. A

26 BTC-e user did not fund an account by directly transferring money to BTC-e itself, but rather users were

27 instructed to wire funds to one of BTC-e's "front" companies that, although nominally separate from

28 BTC-e were, in fact, controlled by and operated for the benefit of BTC-e. Nor could BTC-e users

COMPLAINT   4

1 withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users

2 were required to make withdrawals through the use of third-party "exchangers" or other processors, thus

3 enabling BTC-e to avoid collecting any information about its users that would leave a centralized

4 financial paper trail. Thus, a user could create a BTC-e account with nothing more than a username and

5 email address, which often bore no relationship to the actual identity of the user.

6   20.   BTC-e accounts received criminal proceeds directly from various cybercrimes, including

7 numerous hacking incidents, ransomware payments, identity theft schemes, embezzlement by corrupt

8 public officials, and narcotics distribution. A significant portion of BTC-e's business was derived from

9 suspected criminal activity.

10   21.   Messages on BTC-e's own forum openly and explicitly reflected some of the criminal

11 activity in which the users on the platform were engaged and how they used BTC-e to launder funds.

12 BTC-e users established accounts under monikers suggestive of criminality, including user names such

13 as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire." Despite these

14 suspicious usernames, BTC-e did nothing to identify these customers or to investigate whether these or

15 any of its other customers were using its services to conduct, conceal, or facilitate illegal activity.

16   22.   BTC-e's structure allowed criminals to conduct financial transactions with high levels of

17 anonymity and thereby avoid apprehension by law enforcement or seizure of funds. This aspect of

18 BTC-e contributed to its customers' willingness to accept BTC-e's unfavorable exchange rates

19 compared to other legitimate digital currency exchangers that registered with FinCEN and that had

20 appropriate and effective anti-money laundering and "Know-Your-Customer" policies in place.

21   23.   Customers located within the United States used BTC-e to conduct at least 21,000 bitcoin

22 transactions worth over $296,000,000 and tens of thousands of transactions in other convertible virtual

23 currencies.

24   24.   BTC-e made no effort to register with FinCEN, maintain any elements of an AML

25 program, or report suspicious activity.

26 **C.   Vinnik**

27   25.   Vinnik occupied a senior leadership position within BTC-e and participated in the

28 direction and supervision of BTC-e's operations and finances. Vinnik controlled multiple BTC-e

COMPLAINT   5

1   administrative accounts used to process BTC-e's transactions.

2   26.   The owners and administrators of BTC-e, including Vinnik, were aware BTC-e

3   functioned as a money laundering enterprise. Vinnik sent emails claiming to be an owner of BTC-e and

4   used the site to personally conduct transactions with illegal proceeds.

5   27.   Vinnik operated several administrative, financial, operational, and support accounts at

6   BTC-e, including accounts that have been tied to thefts from other virtual currency exchanges such as

7   Mt. Gox. Furthermore, withdrawals from these accounts were deposited directly into bank accounts tied

8   to Vinnik. These accounts granted Vinnik the ability to observe transactions coming to and leaving

9   from BTC-e, as well as specific customer activity and profiles. Vinnik made no efforts to ensure that

10   BTC-e registered with FinCEN, maintained any elements of an AML program, or reported suspicious

11   transactions.

12   **D.   Indictment**

13   28.   On May 31, 2016, a grand jury sitting in the Northern District of California returned a

14   two-count indictment charging BTC-e and Alexander Vinnik with operation of an Unlicensed Money

15   Services Business, in violation of 18 U.S.C § 1960, and Conspiracy to Commit Money Laundering, in

16   violation of 18 U.S.C. § 1956(h).

17   29.   On January 17, 2017, the grand jury issued a twenty-one count superseding indictment

18   charging BTC-e and Vinnik with Operation of an Unlicensed Money Services Business, in violation of

19   18 U.S.C § 1960; Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h);

20   Money Laundering, in violation of 18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i); and Engaging in

21   Unlawful Monetary Transactions, in violation of 18 U.S.C. § 1957.

22   **E.   FinCEN's Civil Monetary Penalty**

23   30.   As detailed in the Assessment of Civil Money Penalty issued on July 26, 2017 (attached

24   hereto as Exhibit 1), FinCEN assessed monetary penalties against BTC-e and Vinnik for the following

25   conduct:

26   Failure to Register as an MSB

27   31.   A Money Services Business ("MSB") is any person or entity that receives something of

28   value (including currency or value that substitutes for currency) from one person and transmits either the

COMPLAINT   6

1   same or a different form of value to another person or location by any means. 31 C.F.R. §1010.100(ff);

2   2011 MSB Final Rule, 76 FR 43585, at 43596. An MSB is required to register with FinCEN within 180

3   days of beginning operation and to renew such registration every two years. 31 U.S.C. § 5330; 31

4   C.F.R. § 1022.380(b)(2). Foreign-located MSBs that conduct business within the United States must

5   register and must also appoint an agent within the United States to accept legal process in BSA-related

6   matters. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(a)(2).

7   32.   The BTC-e website (btc-e.com) Terms and Conditions contained the following

8   information, "BTC-e provides an online tool that allows users to freely trade Bitcoins for a number of

9   different currencies worldwide." Thus, BTC-e's business model was to transfer something of value –

10   bitcoin and other cryptocurrency – between entities and individuals and between locations. As such,

11   BTC-e was an MSB. At no point in its existence did BTC-e register as an MSB with FinCEN. In

12   March of 2013, FinCEN issued guidance clarifying and affirming its July 2011 Final Rules establishing

13   that exchangers and administrators that transmitted virtual currency and operated in the United States

14   were subject to FinCEN requirements, including registration as an MSB. Nevertheless, BTC-e

15   continued to fail to register.

16   Failure to Establish AML Programs and Procedures

17   33.   Under the BSA, an MSB must develop, implement, and maintain an effective AML

18   program that is reasonably designed to prevent the MSB from being used to facilitate money laundering

19   and the financing of terrorist activities. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a). The

20   AML program must: contain written policies, procedures and internal controls; designate an individual

21   responsible for BSA compliance; provide training, including on how to detect suspicious transactions;

22   and provide for independent review of the AML program. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R.

23   §§ 1022.210(c) and (d).

24   34.   At no point in time did BTC-e have any AML policies or procedures, let alone an

25   effective program for detecting and preventing suspicious transactions. To the contrary, BTC-e's lax

26   policies encouraged persons engaged in criminal activity to use its services, and BTC-e became the

27   virtual currency exchange of choice for criminals looking to launder their illegal proceeds.

28   35.   BTC-e had no policies or procedures to verify customer identification. BTC-e failed to

COMPLAINT   7

1 collect even the most basic customer information needed to comply with the BSA. BTC-e allowed its

2 customers to open accounts and conduct transactions with only a username, password, and e-mail

3 address. BTC-e collected only this limited information no matter how large the transaction or how

4 many transactions the customer conducted. When BTC-e finally implemented policies to verify

5 customer identification in May of 2017, it made those procedures "optional."

6   36.   In fact, BTC-e processed digital currency transactions with features that restricted its

7 ability to identify its customers and detect suspicious activity. For example, BTC-e processed millions

8 of dollars' worth of transactions using bitcoin "mixers." Instead of transmitting bitcoin directly between

9 two users, the "mixer" created layers of temporary bitcoin addresses operated by the mixer itself to

10 complicate any attempt to analyze the flow of the transaction.

11   37.   Moreover, BTC-e had no policies or procedures for conducting due diligence or

12 monitoring transactions for suspicious activity. On some occasions, BTC-e customers contacted BTC-

13 e's administration with questions regarding how to process and access proceeds obtained from the sale

14 of illegal drugs and from transactions on known "darknet" illegal markets, including Silk Road. In

15 addition, BTC-e's customers openly discussed using BTC-e to facilitate illegal activity on BTC-e's own

16 internal messaging system, as well as on its public user chat system. Nevertheless, BTC-e did not

17 implement any policies or procedures to monitor its platform for suspect activity.

18 <div align="center">Failure to File SARs</div>

19   38.   Under the BSA, an MSB must report transactions that the MSB "knows, suspects, or has

20 reason to suspect" are suspicious where those transactions involve the MSB and aggregate to at least

21 $2,000 in value. 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1022.320(a)(2). A transaction is "suspicious" if it

22 (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has

23 no business or apparent lawful purpose; or (d) involves the use of the MSB to facilitate illegal activity.

24 31 U.S.C. § 5318(g)(1); 31 CFR. §§ 1022.320(a)(2)(i)-(iv).

25   39.   Despite the rampant evidence of illegal activity on its platform, BTC-e did not file a

26 single SAR, including for the specific activities identified in the Assessment.

27   40.   On July 26, 2017, FinCEN imposed on BTC-e and Alexander Vinnik civil monetary

28 penalties in the amounts of $88,596,314 and $12,000,000, respectively, for the conduct described above.

COMPLAINT   8

1   *See* Exhibit 1. Defendants have not paid the penalties.

2   **FIRST CAUSE OF ACTION:**
RECOVERY OF CIVIL MONETARY PENALTY

3

4   41.   Plaintiff hereby incorporates by reference each and every allegation set forth in the

5   foregoing paragraphs.

6   42.   The July 26, 2017, Assessment of Civil Money Penalty constitutes a lawful

7   administrative sanction against BTC-e and Vinnik for failure to comply with the BSA's requirements

8   under 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

9   43.   BTC-e is liable to the United States for a civil penalty in the amount of $88,596,314, plus

10   interest and costs.

11   44.   Vinnik is liable to the United States for a civil penalty in the amount of $12,000,000, plus

12   interest and costs.

13   **PRAYER FOR RELIEF**

14   WHEREFORE, Plaintiff respectfully requests that the Court reduce Plaintiff's claims against

15   BTC-e and Alexander Vinnik to judgment, award Plaintiff judgments against BTC-e and Alexander

16   Vinnik in the amounts of $88,596,314 and $12,000,000, respectively, plus interest as provided by law,

17   and award such other relief as the Court deems just and proper, including Plaintiff's costs.

18

19   Dated: July 25, 2019   Respectfully submitted,

20   DAVID L. ANDERSON
United States Attorney

21
                                   /s

22   _____

23   KIRSTIN M. AULT
Assistant United States Attorney

24   Attorneys for United States of America

25

26

27

28

COMPLAINT   9

Exhibit 1

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2017-03**
BTC-E a/k/a Canton Business Corporation	)	
and Alexander Vinnik	)	
	)	

<u>**ASSESSMENT OF CIVIL MONEY PENALTY**</u>

I.   INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to

assess civil money penalties against BTC-E a/k/a Canton Business Corporation (BTC-e) and

Alexander Vinnik, pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that

Act.[1]

FinCEN has the authority to impose civil money penalties on money services businesses

(MSBs) and individuals involved in the ownership or operation of MSBs.[2] Rules implementing the

BSA state that "[o]verall authority for enforcement and compliance, including coordination and

direction of procedures and activities of all other agencies exercising delegated authority under this

chapter" has been delegated by the Secretary of the Treasury to FinCEN.[3]

---

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951–1959 and 31 U.S.C. §§ 5311–5314, 5316–5332.
Regulations implementing the Bank Secrecy Act currently appear at 31 C.F.R. Chapter X.

[2] 12 U.S.C. §§ 1829b(j) and 1955; 31 U.S.C. §§ 5321(a)(1) and 5330(e); 31 C.F.R. § 1010.820.

[3] 31 C.F.R. § 1010.810(a).

BTC-e and Alexander Vinnik have been indicted in the Northern District of California under

18 U.S.C. §§ 1956, 1957, and 1960 for money laundering, conspiracy to commit money laundering,

engaging in unlawful monetary transactions, and the operation of an unlicensed money transmitting

business.[4]

II.   JURISDICTION

BTC-e operates as an "exchanger" of convertible virtual currencies, offering the purchase

and sale of U.S. dollars, Russian Rubles, Euros, Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin,

Ethereum, and Dash.[5] BTC-e also offered "BTC-e code," which enabled users to send and receive

fiat currencies, including U.S. dollars, with other BTC-e users. Since 2011, BTC-e has served

approximately 700,000 customers worldwide and is associated with bitcoin wallet addresses that

have received over 9.4 million bitcoin. Alexander Vinnik participated in the direction and

supervision of BTC-e's operations and finances and controlled multiple BTC-e administrative

accounts used in processing transactions.

Exchangers of convertible virtual currency are "money transmitters" as defined at 31 C.F.R

§ 1010.100(ff)(5) and "financial institutions" as defined at 31 C.F.R § 1010.100(t). A foreign-

located business qualifies as an MSB if it does business as an MSB "wholly or in substantial part

within the United States."[6] Customers located within the United States used BTC-e to conduct at

least 21,000 bitcoin transactions worth over $296,000,000 and tens of thousands of transactions in

other convertible virtual currencies. The transactions included funds sent from customers located

within the United States to recipients who were also located within the United States. In addition,

---

[4] *United States v. BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, CR 16-00227 SI (N.D. CA. Jan. 17, 2017).

[5] FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

[6] 31 U.S.C. §§ 5312(a)(6), 5312(b), and 5330(d); 31 C.F.R. § 1010.100(ff).

these transactions were processed through servers located in the United States. BTC-e attempted to

conceal the fact that it provided services to customers located within the United States. BTC-e

instructed customers to make use of correspondent accounts held by foreign financial institutions or

services provided by affiliates of BTC-e located abroad.

III. DETERMINATIONS

FinCEN has determined that, from November 5, 2011 through the present: (a) BTC-e and

Alexander Vinnik[7] willfully violated MSB registration requirements; (b) BTC-e willfully violated[8]

the requirement to implement an effective anti-money laundering (AML) program, the requirement

to detect suspicious transactions and file suspicious activity reports (SARs), and the requirement to

obtain and retain records relating to transmittals of funds in amounts of $3,000 or more; and (c)

Alexander Vinnik willfully participated[9] in violations of AML program and SAR requirements.[10]

A. **Registration as a Money Services Business**

The BSA and its implementing regulations require the registration of an MSB within 180

days of beginning operations and the renewal of such registration every two years.[11] A foreign-

---

[7] 31 U.S.C. § 5330(a)(1) ("Any person who owns or controls a money transmitting business shall register the business…"); 31 U.S.C. 5330(e)(1) ("Any person who fails to comply with any requirement of [31 U.S.C. § 5330] or any regulation prescribed under [31 U.S.C. § 5330] shall be liable…for a civil penalty…"); 31 C.F.R. § 1022.380(c) ("[A]ny person who owns or controls a money services business is responsible for registering the business…"); 31 C.F.R. § 1022.380(e) ("Any person who fails to comply with any requirement of [31 U.S.C. § 5330 or 31 C.F.R. § 1022.380] shall be liable for a civil penalty…").

[8] 12 U.S.C. § 1829b(j); 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f).

[9] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f) (For any willful violation…of any reporting requirement for financial institutions…, the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who willfully participates in the violation, a civil penalty…).

[10] In civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose.

[11] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(b)(2).

located MSB must appoint an agent who will accept legal process in matters related to compliance with the BSA. [12] The agent must reside within the United States.

At no point in its operations was BTC-e registered with FinCEN. Notably, BTC-e went unregistered even after FinCEN issued guidance pertaining to exchangers and administrators of virtual currency in March 2013. BTC-e never appointed an agent for service of process.

B.   Violations of AML Program Requirements

The BSA and its implementing regulations require an MSB to develop, implement, and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[13] BTC-e was required to implement a written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day to day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program.[14]

BTC-e lacked basic controls to prevent the use of its services for illicit purposes. Through their operation of BTC-e, Alexander Vinnik and other individuals occupying senior leadership positions within the virtual currency exchange attracted and maintained a customer base that consisted largely of criminals who desired to conceal proceeds from crimes such as ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. BSA

---

[12] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(a)(2). *See generally* FIN-2012-A001, "Foreign-Located Money Services Businesses," February 15, 2012.

[13] 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a).

[14] 31 U.S.C. §§ 5318(a)(2) and (h)(1); 31 C.F.R. §§ 1022.210(c) and (d).

compliance was compromised by revenue interests. BTC-e quickly became the virtual currency

exchange of choice for criminals looking to conduct illicit transactions or launder illicit proceeds,

all of which BTC-e failed to report both to FinCEN and law enforcement.

1.   Internal Controls

BTC-e failed to implement policies, procedures, and internal controls reasonably designed to

prevent the MSB from facilitating money laundering. The BSA requires MSBs to implement

policies and procedures to verify customer identification, file BSA reports, create and maintain BSA

records, and respond to law enforcement requests. BTC-e lacked adequate controls to verify

customer identification, to identify and report suspicious activity, and to prevent money laundering

and the financing of terrorist activities. BTC-e offered a variety of convertible virtual currencies

internationally and operated as one of the largest volume virtual currency exchanges. The BSA and

its implementing regulations require an MSB to implement internal controls that are commensurate

with the risks posed by its clientele, the nature and volume of the financial services it provides, and

the jurisdictions in which the MSB provides its services.

BTC-e failed to collect and verify even the most basic customer information needed to

comply with the BSA. BTC-e allowed its customers to open accounts and conduct transactions

with only a username, password, and an email address.   The minimal information collected was the

same regardless of how many transactions were processed for a customer or the amount involved.

BTC-e implemented policies to verify customer identification in May 2017 but stated that

compliance with those policies was "optional."

BTC-e processed transactions with digital currency features that restricted its ability to

verify customer identification or monitor for suspicious activity. BTC-e allowed over $40 million

in transfers on its platform from bitcoin mixers.   Mixers anonymize bitcoin addresses and obscure

bitcoin transactions by weaving together inflows and outflows from many different users. Instead of directly transmitting bitcoin between two bitcoin addresses, the mixer disassociates connections. Mixers create layers of temporary bitcoin addresses operated by the mixer itself to further complicate any attempt to analyze the flow of bitcoin. BTC-e lacked adequate internal controls to mitigate the risks presented by bitcoin mixers.

BTC-e also lacked adequate internal controls to mitigate the risks presented by virtual currencies with anonymizing features. BTC-e facilitated transfers of the convertible virtual currency Dash, which has a feature called "PrivateSend." PrivateSend provides a decentralized mixing service within the currency itself in an effort to enhance user anonymity. BTC-e and Alexander Vinnik failed to conduct appropriate risk-based due diligence to address the challenges anonymizing features would have on compliance with BSA reporting and recordkeeping requirements.

BTC-e lacked adequate procedures for conducting due diligence, monitoring transactions, and refusing to consummate transactions that facilitated money laundering or other illicit activity. Users of BTC-e openly and explicitly discussed conducting criminal activity through the website's internal messaging system and on BTC-e's public "Troll Box," or user chat. This resulted in no additional scrutiny from Alexander Vinnik or BTC-e's other operators and senior leadership. BTC-e received inquiries from customers on how to process and access proceeds obtained from the sale of illegal drugs on darknet markets, including Silk Road, Hansa Market, and AlphaBay.

BTC-e processed transactions involving funds stolen from the Mt.Gox exchange between 2011 and 2014. BTC-e processed over 300,000 bitcoin of these proceeds, which were sent and held at three separate but linked BTC-e accounts. BTC-e failed to conduct any due diligence on the

6

transactions or on the accounts in which the stolen bitcoin were held. Moreover, BTC-e failed to

file any SARs on these transactions even after the thefts were publicly reported in the media.

C.   Failure to File Suspicious Activity Reports

The BSA and its implementing regulations require an MSB to report transactions that the

MSB "knows, suspects, or has reason to suspect" are suspicious, if the transactions are conducted or

attempted by, at, or through the MSB, and the transactions involve or aggregate to at least $2,000 in

funds or other assets.[15] A transaction is "suspicious" if the transaction: (a) involves funds derived

from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or

apparent lawful purpose, and the MSB knows of no reasonable explanation for the transaction after

examining the available facts, including background and possible purpose; or (d) involves use of the

money services business to facilitate criminal activity.[16]

BTC-e processed thousands of suspicious transactions without ever filing a single SAR.

Unreported transactions included those conducted by customers who were widely reported as

associated with criminal or civil violations of U.S. law. For example, from November 14, 2013

through July 21, 2015, BTC-e processed over 1,000 transactions for the unregistered U.S.-based

virtual currency exchange Coin.MX. Coin.MX's operator, Anthony R. Murgio, pled guilty to

charges that included conspiracy to operate an unlicensed money transmitting business.[17] Coin.MX

processed over $10 million in bitcoin transactions derived from illegal activity throughout its

operations, including a substantial number that involved funds from ransomware extortion

---

[15] 31 U.S.C. § 5318(g)(1) and 31 C.F.R. § 1022.320(a)(2).

[16] 31 U.S.C. § 5318(g)(1) and 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv).

[17] "Operator Of Unlawful Bitcoin Exchange Pleads Guilty In Multimillion-Dollar Money Laundering And Fraud Scheme," Department of Justice, U.S. Attorney's Office for the Southern District of New York, January 9, 2017, https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-pleads-guilty-multimillion-dollar-money-laundering.

payments. Even after the conviction of Coin.MX's operator, BTC-e failed to conduct reviews of the transactions that BTC-e processed for Coin.MX and failed to file any SARs.

Criminals, and cybercriminals in particular, used BTC-e to process the proceeds of their illicit activity. This was particularly the case for some of the largest ransomware purveyors, which used BTC-e as a means of storing, distributing, and laundering their criminal proceeds. FinCEN has identified at least $800,000 worth of transactions facilitated by BTC-e tied to the ransomware known as "Cryptolocker," which affected computers in 2013 and 2014. Further, over 40 percent of all bitcoin transactions, over 6,500 bitcoin, associated with the ransomware scheme known as "Locky" were sent through BTC-e. Despite readily available, public information identifying the bitcoin addresses associated with Locky, BTC-e failed to conduct any due diligence on the recipients of the funds and failed to file SARs.

BTC-e also failed to file SARs on transactions that involved the money laundering website Liberty Reserve. Liberty Reserve was a Costa Rica-based administrator of virtual currency that laundered approximately $6 billion in criminal proceeds. Liberty Reserve's website was seized by the U.S. government and shut down when its owner and six other individuals were charged with conspiracy to commit money laundering and operating an unlicensed money transmitting business. FinCEN issued a finding under Section 311 of the USA PATRIOT Act that Liberty Reserve was a financial institution of primary money laundering concern.[18] Not only did BTC-e share customers with Liberty Reserve, "BTC-e code" was redeemable for Liberty Reserve virtual currency. BTC-e failed to file SARs even after the public shutdown of Liberty Reserve in May 2013.

---

[18] "Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311," Department of the Treasury, May 28, 2013, https://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx.

D.   Recordkeeping Requirements

The BSA and its implementing regulations require MSBs and other non-bank financial institutions to obtain and retain records related to transmittals of funds in amounts of $3,000 or more.[19] BTC-e failed to collect even the most basic customer information and lacked adequate procedures for conducting due diligence and monitoring transactions. Transactional records maintained by BTC-e lacked critical information such as name, address, and account numbers.

IV.   CIVIL MONEY PENALTY

FinCEN has determined that BTC-e willfully violated the BSA and its implementing regulations, as described in this ASSESSMENT, and that grounds exist to assess civil money penalties for these violations. FinCEN has determined that the proper penalties in this matter are a penalty of $110,003,314 imposed on BTC-e and a penalty of $12,000,000 imposed on Alexander Vinnik.

By:

_____/s/_____7/26/2017_____
Jamal El-Hindi   Date:
Acting Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury

---

[19] 12 U.S.C. § 1829b and 31 C.F.R. § 1010.410(e).

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

DEFENDANTS

(b) County of Residence of First Listed Plaintiff
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

1   U.S. Government Plaintiff

3   Federal Question
(U.S. Government Not a Party)

2   U.S. Government Defendant

4   Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	1	1	Incorporated *or* Principal Place of Business In This State	4	4
Citizen of Another State	2	2	Incorporated *and* Principal Place of Business In Another State	5	5
Citizen or Subject of a Foreign Country	3	3	Foreign Nation	6	6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
110 Insurance	**PERSONAL INJURY** **PERSONAL INJURY**	625 Drug Related Seizure of Property 21 USC § 881	422 Appeal 28 USC § 158	375 False Claims Act
120 Marine	310 Airplane 365 Personal Injury – Product Liability	690 Other	423 Withdrawal 28 USC § 157	376 Qui Tam (31 USC § 3729(a))
130 Miller Act	315 Airplane Product Liability			400 State Reapportionment
140 Negotiable Instrument	320 Assault, Libel & Slander 367 Health Care/ Pharmaceutical Personal Injury Product Liability	**LABOR**	**PROPERTY RIGHTS**	410 Antitrust
150 Recovery of Overpayment Of Veteran's Benefits	330 Federal Employers' Liability	710 Fair Labor Standards Act	820 Copyrights	430 Banks and Banking
151 Medicare Act	340 Marine 368 Asbestos Personal Injury Product Liability	720 Labor/Management Relations	830 Patent	450 Commerce
152 Recovery of Defaulted Student Loans (Excludes Veterans)	345 Marine Product Liability	740 Railway Labor Act	835 Patent—Abbreviated New Drug Application	460 Deportation
	350 Motor Vehicle **PERSONAL PROPERTY**	751 Family and Medical Leave Act	840 Trademark	470 Racketeer Influenced & Corrupt Organizations
153 Recovery of Overpayment of Veteran's Benefits	355 Motor Vehicle Product Liability 370 Other Fraud	790 Other Labor Litigation	**SOCIAL SECURITY**	480 Consumer Credit
160 Stockholders' Suits	360 Other Personal Injury 371 Truth in Lending	791 Employee Retirement Income Security Act	861 HIA (1395ff)	485 Telephone Consumer Protection Act
190 Other Contract	362 Personal Injury -Medical Malpractice 380 Other Personal Property Damage		862 Black Lung (923)	490 Cable/Sat TV
195 Contract Product Liability		**IMMIGRATION**	863 DIWC/DIWW (405(g))	850 Securities/Commodities/ Exchange
196 Franchise	385 Property Damage Product Liability	462 Naturalization Application	864 SSID Title XVI	
	CIVIL RIGHTS **PRISONER PETITIONS**	465 Other Immigration Actions	865 RSI (405(g))	890 Other Statutory Actions
REAL PROPERTY	440 Other Civil Rights **HABEAS CORPUS**		**FEDERAL TAX SUITS**	891 Agricultural Acts
210 Land Condemnation	441 Voting 463 Alien Detainee		870 Taxes (U.S. Plaintiff or Defendant)	893 Environmental Matters
220 Foreclosure	442 Employment 510 Motions to Vacate Sentence		871 IRS–Third Party 26 USC § 7609	895 Freedom of Information Act
230 Rent Lease & Ejectment	443 Housing/ Accommodations 530 General			896 Arbitration
240 Torts to Land	445 Amer. w/Disabilities– Employment 535 Death Penalty			899 Administrative Procedure Act/Review or Appeal of Agency Decision
245 Tort Product Liability	446 Amer. w/Disabilities–Other **OTHER**			
290 All Other Real Property	448 Education 540 Mandamus & Other			950 Constitutionality of State Statutes
	550 Civil Rights			
	555 Prison Condition			
	560 Civil Detainee– Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

1 Original Proceeding

2 Removed from State Court

3 Remanded from Appellate Court

4 Reinstated or Reopened

5 Transferred from Another District *(specify)*

6 Multidistrict Litigation–Transfer

8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:

Brief description of cause:

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: Yes   No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)   **SAN FRANCISCO/OAKLAND**   **SAN JOSE**   **EUREKA-MCKINLEYVILLE**

DATE   **SIGNATURE OF ATTORNEY OF RECORD**

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. **Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) <u>United States plaintiff</u>. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) <u>United States defendant</u>. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) <u>Federal question</u>. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) <u>Diversity of citizenship</u>. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. **Origin.** Place an "X" in one of the six boxes.

(1) <u>Original Proceedings</u>. Cases originating in the United States district courts.

(2) <u>Removed from State Court</u>. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) <u>Remanded from Appellate Court</u>. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) <u>Reinstated or Reopened</u>. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) <u>Transferred from Another District</u>. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) <u>Multidistrict Litigation Transfer</u>. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) <u>Multidistrict Litigation Direct File</u>. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

<u>Please note that there is no Origin Code 7</u>. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** <u>Example</u>: U.S. Civil Statute: 47 USC § 553. <u>Brief Description</u>: Unauthorized reception of cable service.

VII. **Requested in Complaint.**   <u>Class Action</u>. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

<u>Demand</u>. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

<u>Jury Demand</u>. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. **Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.