DAVID L. ANDERSON (CABN 149604)
United States Attorney

SARA WINSLOW (DCBN 457643)
Chief, Civil Division

KIRSTIN M. AULT (CABN 206052)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6940
FAX: (415) 436-7234
Kirstin.ault@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-e, a/k/a CANTON BUSINESS CORP., and ALEXANDER VINNIK, Defendants.	CASE NO. **COMPLAINT**

The United States of America alleges as follows:

I. NATURE OF ACTION

1. The United States brings this action against BTC-e a/k/a Canton Business Corporation ("BTC-e") and Alexander Vinnik ("Vinnik") (collectively "Defendants"), to recover civil money penalties imposed under the Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §§ 5311-5314 and 5316-5332, which is commonly referred to as the Bank Secrecy Act ("BSA").

II. JURISDICTION AND VENUE

2. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1345. The Court may exercise personal jurisdiction over Defendants because they transact business in this District.

3. Venue is proper in the Northern District of California under 28 U.S.C. §§ 1391(b) and (c) because Defendants transact business in this District.

III. PARTIES

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

5. Defendant BTC-e is a corporation organized under the laws of either Cyprus and/or the Seychelles Islands. BTC-e operated in Bulgaria, the Seychelles Islands, and other jurisdictions, including the Northern District of California. At all times relevant to this complaint, BTC-e was a money services business providing services subject to the BSA in the Northern District of California and elsewhere.

6. Defendant Alexander Vinnik is a Russian national who is currently incarcerated in Greece. At all times relevant to this complaint, Vinnik occupied a senior leadership position within BTC-e.

IV. THE BANK SECRECY ACT

7. The Financial Crimes Enforcement Network ("FinCEN"), a bureau within the United States Department of the Treasury, administers the BSA pursuant to authority delegated by the Secretary of the Treasury. *See* Treasury Order 180-01 (July 1, 2014). The BSA requires the filing of reports and the maintenance of records useful in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

Regulations implementing the BSA appear at 31 C.F.R. Chapter X. Rules issued under the BSA require the registration of money services businesses ("MSBs"), the filing of Suspicious Activity Reports ("SARs"), the implementation of anti-money laundering ("AML") programs, and the maintenance of records related to transmittals of funds.

8. FinCEN may impose a civil monetary penalty "at any time before the end of the 6-year period beginning on the date of the transaction with respect to which the penalty was assessed," and may commence an action to recover the civil money penalty at any time before the end of the 2-year period beginning on the date the penalty was imposed. *See* 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

9. MSBs are "financial institutions" for purposes of the BSA and its implementing regulations. *See* 31 U.S.C. § 5312(a)(2)(J), (K) and (R); 31 C.F.R. § 1010.100(t)(3). A "money services business" is defined in regulations implementing the BSA to include persons who are engaged as a business in providing money transmission services "wholly or in substantial part within the United States." *See* 31 C.F.R. § 1010.100(ff)(5). Exchangers of convertible virtual currency provide "money transmission services" for purposes of regulations implementing the BSA and may therefore qualify as MSBs. *See* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (March 18, 2013).

10. FinCEN may impose on any person who owns or controls an unregistered MSB a civil money penalty for each day that the MSB remains unregistered. *See* 31 U.S.C. § 5330(e)(2); 31 C.F.R. § 1022.380(e). For MSB registration violations occurring on or before November 2, 2015, FinCEN may assess a penalty of up to $7,954 for each violation. 31 C.F.R. § 1010.821. Violations occurring after November 2, 2015, may be assessed in an amount up to $8,084 for each violation. *Id*. Each day a violation continues constitutes a separate violation. 31 C.F.R. § 1022.380(e).

11. FinCEN may impose a civil money penalty on a domestic financial institution that willfully violates the BSA by failing to establish or maintain an adequate AML program and for failing to file SARs as appropriate, and on any partner, director, officer or employee who willfully participates in the violation. *See* 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820. The term "domestic" refers to "the doing of business within the United States" or the performance of functions within the United States. 31 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

a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address. Only the bitcoin address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any information identifying the payer or payee.

16. All bitcoin transactions are recorded on what is known as the Blockchain. The Blockchain is a distributed public ledger that maintains all bitcoin transactions, incoming and outgoing. The Blockchain records every bitcoin address that has ever received a bitcoin and maintains records of every transaction for each bitcoin address. In some circumstances, bitcoin payments may be effectively traced by analyzing the Blockchain.

B. BTC-e Operations

17. BTC-e was a digital currency exchange that allowed users to buy and sell bitcoin, and other digital currencies, anonymously through its web domain btc-e.com. Since its founding, BTC-e has served approximately 700,000 users worldwide, including numerous customers in the United States and in the Northern District of California. BTC-e was used by cybercriminals worldwide and was one of the principal entities used to launder and liquidate criminal proceeds, converting them from digital currencies, including bitcoin, to fiat currencies, including U.S. Dollars, Euros, and Rubles.

18. To use BTC-e, a user created an account by accessing BTC-e's website, www.btc-e.com. To create an account, a user did not need to provide even the most basic identifying information, such as name, date of birth, address, or other identifiers. All BTC-e required to create a user account was a self-created username, password, and an email address. Unlike legitimate digital currency exchangers, BTC-e did not require its users to validate their identity by providing official identification documents. When a customer attempted to use bank wires to transfer funds to or from BTC-e's exchange, BTC-e at times did request identifying documentation, such as a driver's license or passport. BTC-e did not request such documents for all transactions involving bank wires or for other types of transactions.

19. BTC-e's business model obscured and anonymized transactions and sources of funds. A BTC-e user did not fund an account by directly transferring money to BTC-e itself, but rather users were instructed to wire funds to one of BTC-e's "front" companies that, although nominally separate from BTC-e were, in fact, controlled by and operated for the benefit of BTC-e. Nor could BTC-e users

withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were required to make withdrawals through the use of third-party "exchangers" or other processors, thus enabling BTC-e to avoid collecting any information about its users that would leave a centralized financial paper trail. Thus, a user could create a BTC-e account with nothing more than a username and email address, which often bore no relationship to the actual identity of the user.

20. BTC-e accounts received criminal proceeds directly from various cybercrimes, including numerous hacking incidents, ransomware payments, identity theft schemes, embezzlement by corrupt public officials, and narcotics distribution. A significant portion of BTC-e's business was derived from suspected criminal activity.

21. Messages on BTC-e's own forum openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged and how they used BTC-e to launder funds. BTC-e users established accounts under monikers suggestive of criminality, including user names such as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire." Despite these suspicious usernames, BTC-e did nothing to identify these customers or to investigate whether these or any of its other customers were using its services to conduct, conceal, or facilitate illegal activity.

22. BTC-e's structure allowed criminals to conduct financial transactions with high levels of anonymity and thereby avoid apprehension by law enforcement or seizure of funds. This aspect of BTC-e contributed to its customers' willingness to accept BTC-e's unfavorable exchange rates compared to other legitimate digital currency exchangers that registered with FinCEN and that had appropriate and effective anti-money laundering and "Know-Your-Customer" policies in place.

23. 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.

24. BTC-e made no effort to register with FinCEN, maintain any elements of an AML program, or report suspicious activity.

C. Vinnik

25. Vinnik occupied a senior leadership position within BTC-e and participated in the direction and supervision of BTC-e's operations and finances. Vinnik controlled multiple BTC-e

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

26. The owners and administrators of BTC-e, including Vinnik, were aware BTC-e functioned as a money laundering enterprise. Vinnik sent emails claiming to be an owner of BTC-e and used the site to personally conduct transactions with illegal proceeds.

27. Vinnik operated several administrative, financial, operational, and support accounts at BTC-e, including accounts that have been tied to thefts from other virtual currency exchanges such as Mt. Gox. Furthermore, withdrawals from these accounts were deposited directly into bank accounts tied to Vinnik. These accounts granted Vinnik the ability to observe transactions coming to and leaving from BTC-e, as well as specific customer activity and profiles. Vinnik made no efforts to ensure that BTC-e registered with FinCEN, maintained any elements of an AML program, or reported suspicious transactions.

D. Indictment

28. On May 31, 2016, a grand jury sitting in the Northern District of California returned a two-count indictment charging BTC-e and Alexander Vinnik with operation of an Unlicensed Money Services Business, in violation of 18 U.S.C § 1960, and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).

29. On January 17, 2017, the grand jury issued a twenty-one count superseding indictment charging BTC-e and Vinnik with Operation of an Unlicensed Money Services Business, in violation of 18 U.S.C § 1960; Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h); Money Laundering, in violation of 18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i); and Engaging in Unlawful Monetary Transactions, in violation of 18 U.S.C. § 1957.

E. FinCEN's Civil Monetary Penalty

30. As detailed in the Assessment of Civil Money Penalty issued on July 26, 2017 (attached hereto as Exhibit 1), FinCEN assessed monetary penalties against BTC-e and Vinnik for the following conduct:

Failure to Register as an MSB

31. A Money Services Business ("MSB") is any person or entity that receives something of value (including currency or value that substitutes for currency) from one person and transmits either the

same or a different form of value to another person or location by any means. 31 C.F.R. §1010.100(ff); 2011 MSB Final Rule, 76 FR 43585, at 43596. An MSB is required to register with FinCEN within 180 days of beginning operation and to renew such registration every two years. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(b)(2). Foreign-located MSBs that conduct business within the United States must register and must also appoint an agent within the United States to accept legal process in BSA-related matters. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(a)(2).

32. The BTC-e website (btc-e.com) Terms and Conditions contained the following information, "BTC-e provides an online tool that allows users to freely trade Bitcoins for a number of different currencies worldwide." Thus, BTC-e's business model was to transfer something of value – bitcoin and other cryptocurrency – between entities and individuals and between locations. As such, BTC-e was an MSB. At no point in its existence did BTC-e register as an MSB with FinCEN. In March of 2013, FinCEN issued guidance clarifying and affirming its July 2011 Final Rules establishing that exchangers and administrators that transmitted virtual currency and operated in the United States were subject to FinCEN requirements, including registration as an MSB. Nevertheless, BTC-e continued to fail to register.

Failure to Establish AML Programs and Procedures

33. Under the BSA, an MSB must develop, implement, and maintain an effective AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a). The AML program must: contain written policies, procedures and internal controls; designate an individual responsible for BSA compliance; provide training, including on how to detect suspicious transactions; and provide for independent review of the AML program. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. §§ 1022.210(c) and (d).

34. At no point in time did BTC-e have any AML policies or procedures, let alone an effective program for detecting and preventing suspicious transactions. To the contrary, BTC-e's lax policies encouraged persons engaged in criminal activity to use its services, and BTC-e became the virtual currency exchange of choice for criminals looking to launder their illegal proceeds.

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

collect 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 e-mail address. BTC-e collected only this limited information no matter how large the transaction or how many transactions the customer conducted. When BTC-e finally implemented policies to verify customer identification in May of 2017, it made those procedures "optional."

36. In fact, BTC-e processed digital currency transactions with features that restricted its ability to identify its customers and detect suspicious activity. For example, BTC-e processed millions of dollars' worth of transactions using bitcoin "mixers." Instead of transmitting bitcoin directly between two users, the "mixer" created layers of temporary bitcoin addresses operated by the mixer itself to complicate any attempt to analyze the flow of the transaction.

37. Moreover, BTC-e had no policies or procedures for conducting due diligence or monitoring transactions for suspicious activity. On some occasions, BTC-e customers contacted BTC-e's administration with questions regarding how to process and access proceeds obtained from the sale of illegal drugs and from transactions on known "darknet" illegal markets, including Silk Road. In addition, BTC-e's customers openly discussed using BTC-e to facilitate illegal activity on BTC-e's own internal messaging system, as well as on its public user chat system. Nevertheless, BTC-e did not implement any policies or procedures to monitor its platform for suspect activity.

Failure to File SARs

38. Under the BSA, an MSB must report transactions that the MSB "knows, suspects, or has reason to suspect" are suspicious where those transactions involve the MSB and aggregate to at least $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 (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or apparent lawful purpose; or (d) involves the use of the MSB to facilitate illegal activity. 31 U.S.C. § 5318(g)(1); 31 CFR. §§ 1022.320(a)(2)(i)-(iv).

39. Despite the rampant evidence of illegal activity on its platform, BTC-e did not file a single SAR, including for the specific activities identified in the Assessment.

40. On July 26, 2017, FinCEN imposed on BTC-e and Alexander Vinnik civil monetary penalties in the amounts of $88,596,314 and $12,000,000, respectively, for the conduct described above.

See Exhibit 1. Defendants have not paid the penalties.

FIRST CAUSE OF ACTION:
RECOVERY OF CIVIL MONETARY PENALTY

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

42. The July 26, 2017, Assessment of Civil Money Penalty constitutes a lawful administrative sanction against BTC-e and Vinnik for failure to comply with the BSA's requirements under 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court reduce Plaintiff's claims against BTC-e and Alexander Vinnik to judgment, award Plaintiff judgments against BTC-e and Alexander Vinnik in the amounts of $88,596,314 and $12,000,000, respectively, plus interest as provided by law, and award such other relief as the Court deems just and proper, including Plaintiff's costs.

Dated: July 25, 2019

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s

KIRSTIN M. AULT
Assistant United States Attorney

Attorneys for United States of America

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	)	
	)	

ASSESSMENT OF CIVIL MONEY PENALTY

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

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).