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 a 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).