Akin Gump
STRAUSS HAUER & FELD LLP

International Trade Alert

July 31, 2017

Key Points

- On Wednesday, July 27, 2017, FinCEN announced a $110 million fine levied against BTC-e, a digital currency exchange, and a separate $12 million fine against BTC-e's owner, Alexander Vinnick. The fine was due to BTC-e's alleged refusal to abide by AML laws and reporting requirements.
- This was the Treasury's first action against a foreign-located MSB and second against a digital currency exchanger.
- FinCEN publicized that it will work with law enforcement partners around the world to oversee digital currency exchangers and those who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards.

FinCEN Action Demonstrates the Agency's Ability to Use Anti-Money Laundering Laws Against Non-U.S. Entities

Background

On Wednesday, July 27, 2017, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) announced a $110 million fine levied againstBTC-e, a digital currency exchange, forBTC-e's alleged refusal to abide by anti-money laundering (AML) laws and reporting requirements.[1] BTC-e's owner, Russian national Alexander Vinnik, was fined $12 million and arrested in Greece this week for his role in the alleged violations.

BTC-e serves as a virtual currency exchange for Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum and Dash, as well as traditional currencies like the U.S. dollar, the Russian ruble and the euro. The company is headquartered in Russia. Customers have used the service to conduct Bitcoin transactions worth collectively nearly $300 million. BTC-e is currently offline, and a message from company's Twitter account indicates that the site will be down for five to 10 days.

FinCEN's Assessment

FinCEN alleges that BTC-e failed to implement an AML campaign as required by law or to collect and submit suspicious activity reports (SARs), and that Vinnik willfully violated these requirements. The company allegedly ignored flagrant crimes committed using its service, even overlooking discussions of criminal activities taking place on the site's message board. FinCEN also alleges that Vinnik and BTC-e actively courted criminals as a significant customer base, providing near absolute anonymity that the

criminals used to their advantage. The service was used in conjunction with crimes ranging from identity theft and fraud to drug trafficking.

FinCEN further alleges that BTC-e concealed its geographic location and ownership, but it was subject to U.S. AML laws after transacting in funds sent from customers located within the United States and to recipients located in the United States. In its press release, FinCEN stated in part:

"This action should be a strong deterrent to anyone who thinks that they can facilitate ransomware, dark net drug sales, or conduct other illicit activity using encrypted virtual currency. Treasury's FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards."

To abide by AML laws, a money services business (MSB) must register with FinCEN, implement an AML compliance program, report suspicious activities, and keep and share certain records. When suspicious activity is detected, MSBs must submit SARs. A transaction is deemed potentially "suspicious" if it has no apparent business or lawful purpose and is more than $2,000. According to FinCEN, BTC-e allowed thousands of suspicious transactions without ever filing a SAR. BTC-e also processed transactions involving funds stolen from Mt. Gox, one of the largest Bitcoin exchanges. BTC-e facilitated at least $3 million in transactions tied to ransomware attacks. Finally, BTC-e shared customers and conducted transactions with Liberty Reserve, a now-defunct money laundering website that was subject to a FinCEN Section 311 finding identifying it as a financial institution of primary money laundering concern.

Related Arrest of Mr. Vinnik

A group of U.S. law enforcement agencies, including the Department of Justice, Internal Revenue Service, Immigration and Customs Enforcement, Federal Bureau of Investigation, United States Secret Service, Federal Deposit Insurance Corporation and FinCEN, announced that Mr. Vinnik was arrested in Greece to face charges in the United States.[2] The indictment describes Mr. Vinnik, a Russian citizen, as the owner and operator of multiple BTC-e accounts and the primary beneficial owner of BTC-e's managing shell company, Canton Business Corporation. The indictment alleges that Mr. Vinnik received funds from the "hack" of Mt. Gox and subsequently laundered those funds through BTC-e and other online exchanges.

In part, U.S. Attorney Stretch stated, "This office will continue to devote the necessary resources to ensure that money launderers and cyber-criminals are detected, apprehended, and brought to justice wherever and however they use the internet to commit their crimes."

The indictment charges BTC-e and Vinnik with one count of operation of an unlicensed money service business, in violation of 18 U.S.C. § 1960, and one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h). In addition, the indictment charges Mr. Vinnik with 17 counts of money laundering, in violation of 18 U.S.C. § 1956(a)(1), and two counts of engaging in unlawful monetary

transactions, in violation of 18 U.S.C. § 1957. An indictment merely alleges that crimes have been committed, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt.

Conclusions

This penalty follows FinCEN's January 2017 assessment of $184 million against another MSB—making FinCEN's penalties against MSBs this year more than $306 million and, for all entities this year, $314 million total. These penalties represent a significant increase over 2016 penalties, which totaled approximately $11.8 million. They also represent a higher proportion of actions against MSBs versus other regulated financial institutions like banks or casinos (i.e., two of three in 2017 versus one of six in 2016).

MSBs represent a wide range of entities, including money transmitters and exchangers like BTC-e, but also providers of prepaid access (e.g., gift cards) and dealers in foreign exchange. They can be treated as high-risk accounts by traditional banks, already subject to additional scrutiny and diligence. This penalty may dampen the recent surge in investments in digital currencies, with the reminder that FinCEN is willing to go after these services when they fail to abide by AML and reporting requirements, and due to the high-risk activities in which these entities may be engaged. It also underscores FinCEN's reach outside of the United States.

Entities that are MSBs, that work with MSBs or that are considering engaging in virtual currencies should carefully evaluate their AML compliance programs. This includes assessing the efficacy of internal audits and risk assessments, customer identification programs, due diligence on beneficial owners and related accounts, and SAR management. Additionally, MSBs that operate outside of the United States should identify connections to the United States, such as customers or recipients and assess how U.S. AML regulations apply to their business.

Contact Information

If you have any questions concerning this alert or your compliance program, please contact:

Jonathan C. Poling
jpoling@akingump.com
+1 202.887.4029
Washington, D.C.

Anne E. Borkovic
aborkovic@akingump.com
+1 202.887.4432
Washington, D.C.

[1] FinCEN's penalty assessment and press release are available here and here.

[2] The Department of Justice's press release is available here.