Legal Sidebar

For First Time, FinCEN Imposes Penalty on Foreign-Based Virtual Currency Exchange for Violations of Anti-Money Laundering Laws

08/17/2017

On July 26, 2017, Treasury's Financial Crimes Enforcement Network (FinCEN) announced an enforcement action that may signal the agency's growing interest in joining forces with other federal and international law enforcement authorities to investigate foreign-based virtual currency exchanges and hold them accountable when their activities violate U.S. laws. FinCEN issued an Assessment of Civil Money Penalty imposing penalties of $110 million against BTC-e a/k/a Canton Business Corporation (BTC-e) and $12 million against its Russian owner-operator, Alexander Vinnik. The assessment against BTC-e was FinCEN's first enforcement action against a foreign-based virtual currency exchange in which the agency relied on transactions conducted for U.S. customers as its basis for jurisdiction. Simultaneously with FinCEN's announcement, Greek authorities arrested Mr. Vinnik, and the U.S. Attorney for the Northern District of California unsealed a January 17, 2017, indictment charging him and BTC-e with money laundering.

As background, under the Bank Secrecy Act (BSA) and its implementing regulations, "money services businesses" (MSBs) must – among other requirements – (1) register with FinCEN; (2) develop, implement, and maintain an effective anti-money laundering (AML) program; (3) detect and report suspicious activity to FinCEN; and (4) maintain records relating to transmittals of funds in amounts of $2,000 or more. Pursuant to a 2011 FinCEN regulation, a foreign-based business qualifies as an MSB if it does business "wholly or in substantial part in the United States," when "persons in the United States are obtaining MSB services" by "sending money to or receiving money from third parties" through the foreign-based entity. And in 2013, FinCEN issued guidance that any virtual currency "exchanger" (i.e., an entity engaged in the buying and selling of both fiat money (e.g., U.S. dollars and Russian rubles) and virtual currency (e.g., bitcoin and litecoin) will be considered a "money transmitter", which is a type of MSB. As a result, the 2013 regulations subject virtual currency exchangers to the requirements of the BSA and its implementing regulations.

To date, FinCen has taken two enforcement actions against virtual currency exchanges. In 2013, FinCEN issued a proposed regulation eliminating access to the U.S. financial system for the now-defunct Costa-Rican based virtual currency administrator, Liberty Reserve. And in 2015, FinCEN assessed a civil money penalty of $700,000 against Ripple Lab, a virtual currency exchange incorporated in Delaware and headquartered in California. However, the BTC-e action is novel because it marks the first time FinCEN has taken an enforcement action against a foreign-based virtual currency exchanger based on the MSB's business in the United States.

According to FinCEN, BTC-e's operations, as revealed by a multi-agency federal investigation, satisfied FinCEN's definition of MSB because, while BTC-e was based overseas, it handled transactions for customers in the United States that involved millions of dollars' worth of bitcoin and other virtual currencies, including transactions worth nearly $300 million that began and ended in the United States. As a result, FinCEN cited BTC-e for failing to comply with the regulations requiring MSB registration, record-keeping, anti-money laundering programs, and suspicious activity reporting. Examples of FinCEN's assessment of BTC-e's inadequacies include:

- BTC-e had no procedures in place to verify customer identity. Rather than assessing the risk presented by customers based on volume or amount of transactions, BTC-e required only the same minimal amount of information from every customer. Moreover, BTC-e took transactions from third-party bitcoin-mixing services

that should have been rejected because these services provide bitcoin users a means of further hiding their identity by layering transactions.

- BTC-e had no established policies and controls in place to prevent its facilities from being used to facilitate criminal activity. This failure, according to FinCEN, might have contributed to BTC-e's transmitting $800,000 tied to a fraud involving the 2013-2014 "Cryptolocker" ransomware computer attacks.

- BTC-e never filed any Suspicious Activity Reports (SARs) despite having processed thousands of transactions that should have been flagged as suspicious. According to FinCEN, BTC-e processed $10 million in transactions (including some ransomware extortion transactions) for Coin.MX, an unlicensed virtual currency exchange, whose operator pled guilty to federal money laundering charges. BTC-e also failed to file SARs on transactions involving Liberty Reserve's virtual currency, both before and after FinCEN had issued a finding identifying Liberty Reserve to be a financial institution "of primary money laundering concern" under Section 311 of the USA Patriot Act.

Fin-CEN's enforcement efforts against BTC-e could be of importance to the future of virtual currency exchanges around the globe and to those in Congress interested in regulating such exchanges. In moving against BTC-e, FinCEN may be signaling to virtual currency exchanges, both here and abroad, that they should be diligent in observing U.S. anti-money laundering (AML) requirements that prevent users of virtual currency from conducting transactions anonymously. Moreover, the inadequacies FinCEN identified in BTC-e's operation are likely to serve as compliance guidance for other foreign-located virtual currency exchanges that handle transactions for U.S. customers.

FinCEN's efforts to regulate foreign-based virtual currency operations and prevent them from being a tool of terrorists and criminals may be of congressional interest. According to a recent study, AML controls to track transactions are required to mitigate the risk that terrorist networks will become widespread users of digital currencies. Assessing that risk has garnered attention from two congressional committees. On May 16, 2017, the House Committee on Homeland Security reported a bill, H.R. 2433, that would require the Department of Homeland Security to assess the threat posed by terrorist use of virtual currency. The House Financial Services Subcommittee on Terrorism and Illicit Finance held hearings on June 8 and July 18 that explored, among other things, the exploitation of virtual currency by terrorists and transnational criminal groups.

Posted at 08/17/2017 09:33 AM