GT GreenbergTraurig

Alert | Blockchain/Financial Regulatory & Compliance

May 2020

FinCEN Director Confirms Enforcement Focus on Virtual Currency AML Compliance

As another sign of the times, but arguably quite apt given the subject matter, the Consensus Blockchain Conference convened virtually in 2020, with Financial Crimes Enforcement Network (FinCEN) Director Ken Blanco delivering prepared remarks to the conference on May 13, 2020. In those remarks, Blanco confirmed that FinCEN and other federal authorities are focused on financial crimes involving virtual currency, and in particular on whether virtual currency service providers are meeting their obligations to identify and report such activity.

FinCEN is the primary regulator and administrator of the Bank Secrecy Act (BSA), which imposes certain record-keeping, reporting, and other anti-money laundering (AML) compliance obligations on financial institutions, including money services businesses (MSBs) that transact in virtual currency. Federal authorities had previously signaled an increased focus on AML compliance in the virtual currency space. But Blanco's remarks at the Consensus Blockchain Conference were perhaps the most explicit articulation of that enforcement focus to date.

In particular, Blanco indicated that:

> [FinCEN] expect[s] each financial institution to have appropriate controls in place based on the products or services it offers, consistent with the obligation to maintain a risk-based AML program. **This means we are taking a close look at the AML/CFT controls you put on**

> **the types of virtual currency you offer**—whether it be Monero, Zcash, Bitcoin, Grin, or something else—**and you should too**.

In addition, Blanco identified cybercrime as a high priority for federal authorities in the COVID-19 environment, noting that "cybercriminals predominantly launder their proceeds and purchase the tools to conduct their malicious activities via virtual currency." Blanco reminded virtual currency service providers to remain alert to malicious or fraudulent transactions related to, or opportunistically facilitated by, the current pandemic, which must be reported to federal authorities through the filing of suspicious activity reports (SARs). Blanco encouraged companies to include identifying cyber data in their SARs, including Internet Protocol (IP) addresses, malware hashes, malicious domains, and virtual currency addresses associated with ransomware or other illicit transactions.

Blanco also highlighted FinCEN's concern about the AML risks posed by businesses outside the United States that are engaged in money transmission with U.S. customers but are not registered/licensed by FinCEN. This was one of the red flags for virtual currency abuse that FinCEN identified in its May 2019 Advisory on that topic.

Although his remarks sounded a warning to companies that may have been neglecting their AML compliance obligations, Blanco also struck a collaborative tone, noting that FinCEN's "partnerships with industry are paramount in the virtual currency space." Among the areas ripe for public-private collaboration, according to Blanco, is the effective implementation of FinCEN's Travel Rule – the expectation that financial institutions identify counterparties involved in transactions. While that expectation has provoked significant consternation among some digital currency service providers, Blanco expressed confidence that companies would find "creative solutions" to any barriers to compliance, and invited collaboration with FinCEN on that score.

Author

This GT Alert was prepared by:

- Kyle R. Freeny ‡ | +1 202.331.3118 | freenyk@gtlaw.com

‡ Admitted in California. Practice in the District of Columbia limited to matters and proceedings before Federal courts and Agencies.