Published on *The National Law Review* https://natlawreview.com

AML Compliance Scrutiny of Virtual Currency Services in 2020 and Beyond

Article By:

Kyle R. Freeny

In the last decade, traditional financial institutions such as banks and broker-dealers have faced increased scrutiny from federal regulators and prosecutors related to the adequacy of their anti-money laundering (AML) compliance programs. Until recently, however, the federal government's enforcement efforts against cryptocurrency exchange platforms and other virtual currency firms subject to the Bank Secrecy Act (BSA), 31 U.S.C. § 5311 *et seq*., were relatively limited. Recent developments suggest that the days of this limited focus may be over and that federal authorities may now be positioning themselves to scrutinize the adequacy of digital financial firms' AML compliance programs in 2020 and beyond.

In 2013, FinCEN issued interpretive guidance to clarify that the AML compliance obligations mandated by the BSA apply to companies involved in the transmission or exchange of convertible virtual currencies (CVCs), just as they do to more traditional money services business (MSBs).[1] This includes the requirement to file suspicious activity reports ("SARs") to alert federal law enforcement of customer transactions that may indicate illicit activity and the requirement to implement and maintain an effective anti-money laundering program targeted at identifying and mitigating the risk that the company's services will be exploited by criminals.

In the years that immediately followed FinCEN's 2013 interpretive guidance, FinCEN and the Department of Justice (DOJ) focused their enforcement efforts on what might be characterized as the low-hanging fruit of digital AML compliance, namely, virtual currency exchangers that (1) that entirely failed to register with FinCEN, as required, or (2) that operated or facilitated so-called "darknet" markets for illicit goods and services and were thereby directly complicit in money laundering.

More recently, however, FinCEN and other federal authorities, including the Department of Justice, have signaled that they expect more from virtual currency exchanges than mere licensure and non-complicity in criminal acts; they expect implementation of compliance programs that are adequately tailored to the specific AML risks posed by digital assets.

One of the first signals of this shift in focus came in May 2019, when FinCEN issued an advisory on the unique AML risks posed by virtual currencies.[2] In that advisory, FinCEN advised that entities subject to the BSA "should carefully assess and mitigate any potential money laundering, terrorist financing, and other illicit financing risks associated with" virtual currency. The advisory went on to

detail specific red flags for virtual currency abuse that financial institutions should be on the lookout for. These red flags included the use of mixers and tumblers to obscure the provenance of funds, as well as transaction activity consistent with the operation of an unregistered peer-to-peer (P2P) exchange. In the months following issuance of the advisory, FinCEN reported an increase—totaling more than 11,000—in SAR filings from virtual currency service providers like exchanges and kiosks.[3]

Then, in February 2020, Treasury issued an updated National Illicit Finance Strategy (2020 Treasury Strategy), which identified key vulnerabilities in the U.S. financial system in order to guide the deployment of AML enforcement resources within the federal government.[4] One of the key sources of vulnerability identified in the report was the misuse of digital assets. Like the May 2019 FinCEN advisory, the Treasury 2020 Strategy highlighted the heightened potential AML risks posed by anonymity-enhanced currencies.

The focus on digital assets in the 2020 Treasury Strategy is supported by recent capacity building among regulators and DOJ. The SEC's hiring in 2018 of a digital currency "czar" was widely reported. Garnering lesser attention but no less significant, DOJ's Money Laundering and Asset Recovery Section (MLARS) also now has a permanent "Digital Currency Counsel," responsible for coordinating enforcement and increasing capacity throughout DOJ in this area.

In light of these developments, firms that transact in digital assets may wish to evaluate their exposure to the unique AML risks posed by digital assets and ensure that proper internal controls are in place to respond to shifting risks in this emerging area, paying particular attention to the red flags identified by FinCEN. Because the 2020 Treasury Strategy also identifies money services businesses (MSBs) as a separate vulnerability to AML risk, digital MSBs, including digital currency exchanges and payment processors,[5] should pay attention to their compliance obligations in 2020 and beyond.

The need to mitigate the risks posed by virtual currency transactions is not limited to Fintech companies, however. In remarks delivered to the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference in December 2019, FinCEN director Kenneth Blanco advised that all financial institutions, not just virtual currency platforms, may "need to reevaluate whether their institutions are exposed to cryptocurrency."[6] Given the heightened enforcement attention being paid to the Fintech space, coupled with the increased penetration by virtual currency into traditional financial spheres, banks and other traditional financial firms should evaluate third-party business relationships and identify touchpoints with high-risk virtual currency transactions to ensure an adequate risk-based response.

In sum, scrutiny of virtual currencies may increase in 2020 and beyond. For companies operating in this space, the challenges of operating legally are not only relatively novel but are increasingly more complex. At the same time, the current moment offers a unique window of opportunity for companies to help shape policy in this area, as enforcement authorities continue to grapple with how to fit emerging technologies into existing AML frameworks. The 2020 Treasury Strategy explicitly encourages public-private communication as a key priority for mitigating AML risk. Forward-leaning companies may wish not only to carefully evaluate their compliance programs using the traditional BSA protocols, but also to consider the possibility of engagement with enforcement authorities to ensure that emerging enforcement policy in this space accommodates new technological and business realities.

---

[1] FinCEN, A*pplication of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013).

[2] FinCEN, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019).

[3] *See* Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference (Blanco Remarks) (Dec. 10, 2010).

[4] Dep't of Treasury, National Strategy for Combating Terrorist and Other Illicit Financing (2020)

[5] According to FinCEN, although the BSA generally exempts "payment processors" from its AML compliance program obligations, the provision of payment processing services through digital currency transmission "generally is unable to satisfy" the conditions for qualification as a "payment processor" under the BSA, because "such money transmitters do not operate . . . through clearing and settlement systems that only admit BSA-regulated financial institutions as members." *See* FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 at 21 (May 9, 2019).

[6] Blanco Remarks (Dec. 10, 2010).

National Law Review, Volume X, Number 132