Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 2 /JULY 2, 2015

EXPERT ANALYSIS

Criminalizing Free Enterprise: The Bank Secrecy Act and The Cryptocurrency Revolution

By Jeffrey Alberts, Esq., and Leighton Dellinger, Esq.
Pryor Cashman

Over the past several years, financial technology companies (also known as fintech companies) have been using bitcoin and other cryptocurrencies to challenge traditional banking models and offer new financial products that cut costs and increase market efficiency. The power of cryptocurrency technology has become so widely recognized that large companies such as Dell and Time Inc. accept cryptocurrency payments, and cryptocurrency technology will soon be used by Nasdaq to handle pre-IPO trading among private companies.[1]

However, strict enforcement of anti-money-laundering statutes and regulations that were drafted to apply to larger, traditional financial institutions threaten to put the brakes on fintech developments that use cryptocurrencies.

It has been widely reported that prosecutors and financial regulators have been using criminal penalty provisions of the Currency and Foreign Transactions Reporting Act of 1970, 18 U.S.C. § 5318, which is commonly known as the Bank Secrecy Act, to extract massive penalties from global banks. The statute's criminal provisions have also been applied to smaller financial institutions, and there is good reason to believe they will be applied to fintech companies that use cryptocurrencies.

Bank Secrecy Act enforcement is an important bulwark against money laundering, but it also imposes expensive and onerous anti-money-laundering monitoring and reporting requirements. In addition, it carries serious criminal penalties for violations. This commentary explains how the Bank Secrecy Act can be applied to fintech companies that use cryptocurrencies, summarizes recent enforcement trends and discusses steps that fintech companies can take to avoid criminal liability under the act.

THE BANK SECRECY ACT AND CRYPTOCURRENCIES

The Bank Secrecy Act sets forth rules for banks and other financial institutions, including money services businesses, to detect and report suspicious financial transactions to law enforcement and regulatory agencies.

These protocols include registration with the U.S. Treasury Department's Financial Crimes Enforcement Network and regular monitoring and reporting of suspicious transactions through suspicious activity reports to FinCEN.

Failure to comply with Bank Secrecy Act protocols carries severe criminal penalties: Willful violators are subject to a criminal fine of up to $250,000 and/or five years in prison. These maximum penalties double for anyone who commits such a violation while violating another U.S. law or engaging in a pattern of criminal activity.

Remarkably, a separate violation occurs for each day that a violation continues — meaning that millions of dollars and decades of prison time can accumulate in the space of a few days.[2]

A fintech company that uses cryptocurrency can become subject to the Bank Secrecy Act if it qualifies as a money services business. Acting as a money transmitter in a business qualifies an entity as money services business, unless an exemption applies. FinCEN has concluded that a cryptocurrency, or "virtual currency," is a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency.

In evaluating whether a participant in a virtual currency transfer is a money transmitter, FinCEN has used the categories of "user," "exchanger" and "administrator":

- A user is a person or entity that obtains virtual currency to purchase goods or services.
- An exchanger is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency.
- An administrator is a person or entity engaged as a business in issuing (putting into circulation) a virtual currency and has the authority to redeem (to withdraw from circulation) such virtual currency.

A user who merely uses convertible virtual currency to purchase real or virtual goods or services is not a money services business.

A fintech company that makes use of cryptocurrency can become subject to the Bank Secrecy Act if it qualifies as a money services business.

However, an exchanger or administrator who accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from that designation applies.[3]

Companies categorized as money services businesses bear the responsibility and costs of Bank Secrecy Act compliance. Compliance is costly, and for an entity that does not have compliance expertise it is also difficult.

For example, money services businesses that provide money transfer services must obtain and record specific information for each transfer of $3,000 or more, regardless of the method of payment. For record-keeping purposes, the money services business must:

- Verify customer identification.
- Record customer and transaction information.
- Receive certain information from money senders.
- Keep the record for five years from the date of the transaction.

In addition to these general record-keeping requirements, money services businesses have monitoring and reporting obligations that include setting up systems for identifying and reporting suspicious transactions.[4]

Given that fintech startups often have only a handful of employees (sometimes with no regulatory experience) and have limited operating capital, being categorized as a money services business often creates compliance burdens that are difficult to shoulder. In addition, companies that fail to recognize they are subject to regulation as money services businesses may face harsh criminal penalties.

How prosecutors and regulators choose to enforce the Bank Secrecy Act can therefore determine the viability of a fintech company. A broad interpretation of the scope of the Bank Secrecy Act, coupled with strict criminal enforcement, would threaten the entire virtual currency sector — which is heavily involved in developing systems for transferring value and depends on mechanisms for exchanging fiat currency (such as U.S. dollars) for virtual currency (such as bitcoin).

USE OF BANK SECRECY ACT AGAINST BANKS

In recent years, the federal government has repeatedly charged banks with violating the Bank Secrecy Act. Moreover, many of these actions included criminal charges for failing to maintain an effective anti-money-laundering program, as required under 31 U.S.C. § 5318(h), or failing to file a suspicious activity report, as required under 31 U.S.C. § 5318(g). This is particularly noteworthy, because under these provisions it is not necessary for the government to prove that a financial institution actually laundered money to obtain a conviction. Instead, it is sufficient to establish that the financial institution willfully failed to maintain an effective anti-money-laundering program or to report a suspicious transaction.

For example, in 2014, the U.S. attorney for the Southern District of New York charged JPMorgan with two felony violations of the Bank Secrecy Act relating to its relationship with Bernard L. Madoff Investment Securities. The alleged felonies did not include money laundering. Rather, the government charged JPMorgan with failing to maintain an effective anti-money-laundering program and failing to file a suspicious activity report. JPMorgan agreed to pay more than $2 billion to resolve these charges and claims for civil money penalties.[5]

Similarly, in 2012, the U.S. attorney for the Eastern District of New York charged HSBC Group with four felony violations relating to transactions conducted on behalf of its customers in Cuba, Iran, Libya, Sudan and Myanmar. The alleged felonies again included failing to maintain an effective anti-money-laundering program and failing to file suspicious activity reports. HSBC Group agreed to forfeit $1.25 billion in assets and to pay an additional $665 million in penalties to resolve these charges.[6]

While the massive penalties imposed against the largest banks have grabbed the headlines, smaller banks and financial institutions have also faced penalties for alleged violations of the Bank Secrecy Act. For example, in 2012, the Department of Justice charged Moneygram International Inc. with felonies including failing to maintain an effective anti-money-laundering program. Moneygram agreed to forfeit $100 million to resolve the charges.[7]

Similarly, in 2011, the U.S. attorney in the Southern District of Florida charged the privately owned Ocean Bank with failing to establish an effective anti-money-laundering program. Ocean Bank agreed to forfeit more than $10 million to resolve the charges.

The government can obtain a conviction by showing the financial institution willfully failed to maintain an effective anti-money-laundering program or failed to report a suspicious transaction.

VIRTUAL CURRENCY

Over the past two years, FinCEN has issued a formal guidance and several administrative rulings concerning the application of the Bank Secrecy Act to virtual currency companies.[8] It is therefore not surprising that in May FinCEN brought its first civil enforcement action against a virtual currency exchanger.

In that action, FinCEN claimed the exchanger violated the Bank Secrecy Act by acting as an money services business without registering with FinCEN or maintaining an adequate anti-money-laundering program. The exchanger agreed to pay a fine of $700,000 and implement an enhanced Bank Secrecy Act compliance program. The enhancements include a three-year look back period, during which the company will review prior suspicious transactions and file suspicious activity reports with the regulators, and retention of an independent, external auditor that will conduct biannual reviews of the company's Bank Secrecy Act compliance program through 2020.[9]

In a public address given the day after the civil money penalty was announced, FinCEN Director Jennifer Shasky Calvery emphasized the agency's focus on virtual currency companies.

"Virtual currency exchangers — like all members of regulated industry — must bring products to market that comply with our anti-money-laundering laws," she said. "Innovation is laudable but only as long as it does not unreasonably expose our financial system to tech-smart criminals eager to abuse the latest and most complex products."[10]

FinCEN brought its first civil enforcement action against a virtual currency exchanger in May.

Calvery made it clear that FinCEN's scrutiny of the virtual currency industry was just beginning, noting that the agency "recently launched a series of supervisory examinations of businesses in the virtual currency industry."

Initiating supervisory examinations of this newly formed industry is likely to result in additional enforcement actions, because virtual currency companies are still struggling to understand Bank Secrecy Act rules and regulations and how they apply to virtual currency transactions.

AVOIDING LIABILITY

Virtual currency companies that are concerned that they may face civil penalties, or even criminal enforcement, for Bank Secrecy Act violations can take measures to comply with the law and avoid exposure to criminal liability. The threshold question for each of these companies is whether it is a "money services business" as defined by FinCEN.

As noted above, this analysis begins by assessing whether the company qualifies as an "administrator" or "exchanger." Answering these preliminary questions is often difficult, because many businesses that do not view themselves as administrators or exchangers fall within FinCEN's broad definitions. Moreover, companies that fall within the categories of administrator or exchanger sometimes qualify for exemptions to money services business status.

For example, even if a company otherwise meets the criteria for being an administrator or exchanger, it is not a money services business if it "[a]ccepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds."[11]

An even more important question, which is often overlooked by founders of fintech companies, is whether company operations can be altered so as to avoid application of the Bank Secrecy Act. Many fintech companies try to maximize the functionality of the financial services they offer to make their services as consumer-friendly as possible.

For example, a company operating a virtual currency platform may seek to include the ability to exchange fiat currency for virtual currency even though this is not a core function of the service that it provides. This instinct, which is understandable and even laudable from the perspective of maximizing customer satisfaction, can unnecessarily generate Bank Secrecy Act compliance obligations that dramatically outweigh the benefit of expanding the company's service offerings.

It is often in the interest of fintech companies to tailor their services to focus on their strengths and avoid compliance burdens. The sooner a fintech company focuses on this issue, the easier it is to adjust the company's operation to minimize regulatory costs, maximize profitability and stay out of jail.

NOTES

[1] *See* Bradley Hope & Michael J. Casey, *A Bitcoin Technology Gets Nasdaq Test*, WALL ST. J., May 10, 2015; Sydney Ember, *Time Inc. Begins Accepting Bitcoin Payments*, N.Y. TIMES, Dec. 16, 2014.

[2] 18 U.S.C. § 5322.

[3] *See* Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, Fin-2013-G001 (Mar. 18, 2013).

[4] *See* FinCEN, Bank Secrecy Act Requirements, A Quick Reference Guide for Money Services Businesses, *available at* http://1.usa.gov/1LAfXoY.

[5] *See* Press Release, FinCEN, JPMorgan Admits Violation of the Bank Secrecy Act for Failed Madoff Oversight; Fined $461 Million by FinCEN (Jan. 7, 2014), http://1.usa.gov/1U4leJ2.

[6] Press Release, U.S. Dep't of the Treasury, Treasury Department Reaches Landmark Settlement with HSBC (Dec. 11, 2012), http://1.usa.gov/1CH0Rqo.

[7] Press Release, Dep't of Justice, Moneygram International Inc. Admits Anti-Money Laundering and Wire Fraud Violations, Forfeits $100 Million in Deferred Prosecution (Nov. 9, 2012), http://1.usa.gov/1RgMp1K. In addition, in 2014, the U.S. attorney in the Southern District of New York sued the former chief compliance officer of Moneygram for violating the Bank Secrecy Act. *See* Press Release, Dep't of Justice, Manhattan

U.S. Attorney Sues Thomas E. Haider, Former Chief Compliance Officer of Moneygram International Inc. for Violating the Bank Secrecy Act (Dec. 18, 2014), http://1.usa.gov/1HsnHaT.

[8] Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, Fin-2013-G001 (Mar. 18, 2013); Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014); Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014); Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, FIN-2014-R011 (Oct. 27, 2014); Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014).

[9] *See* Press Release, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), http://1.usa.gov/1RQcYZk.

[10] Jennifer Shasky Calvery, Director, FinCEN, Speech at West Coast AML Forum (May 6, 2015), *available at* http://1.usa.gov/1zN2kQ6.

[11] 31 C.F.R. § 1010.100(ff)(5)(ii)(F).

Jeffrey Alberts (L), head of the white collar defense and investigations practice at **Pryor Cashman** based in New York, is a former assistant U.S. attorney in the Southern District of New York. **Leighton Dellinger** (R) is an associate in the firm's litigation, intellectual property, and media and entertainment groups, where she prosecutes and defends against complex commercial, entertainment and intellectual property cases.