WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Should You Bank a Virtual Currency Business?

Written By Lance P. Martin (lpm@wardandsmith.com)
September 28, 2018

Virtual currencies like Bitcoin and Ethereum have spawned many types of businesses that need banking services.

Many banks "de-risk" -- do not provide banking services -- to these businesses. Many virtual currency businesses are regulated as "money services businesses" ("MSBs") under Anti-Money Laundering ("AML") laws because, though virtual currencies are not currencies under these laws, "money transmission services" include business that accept or transmit currency or funds "or other value that substitutes for currency."

A traditional MSB handles remittances in ordinary currency for unbanked or underbanked customers. Some of these traditional MSBs are large operations like MoneyGram. Others are "mom and pop" stores. Most banks have de-risked *traditional* MSBs that handle ordinary currency transmissions. Regulatory agencies wish to see more banks extend services to traditional MSBs, but nevertheless impose a daunting regulatory burden on depository institutions doing so.

Virtual currencies present an additional layer of risk, discussed more fully below, and this added risk will cause many if not most banks to be reluctant to offer banking services to virtual currency MSBs. Any financial institutions that decide to bank virtual currency MSBs must design and implement comprehensive AML and related policies specifically tailored to address unique virtual currency issues.

Virtual Currency Basics

Virtual currencies are electronic representations of value that may or may not have an equivalent value in a real government-backed currency. A virtual currency can be used as a payment system, or digital currency, without an intermediary like a bank or credit card company. Although virtual currencies can function like real currencies in certain transactions, and some virtual currencies can be exchanged for real currencies, a virtual currency itself does not have legal tender status.

Virtual currencies operate using distributed-ledger technology. This technology is called the blockchain. The blockchain eliminates the need for intermediaries such as banks. The blockchain ledger is both transparent and opaque. It is transparent as to the ownership chain of every item of virtual currency. In this way, it is easier to “trace” a virtual currency than to trace cash, and this feature actually assists law enforcement. But the blockchain represents ownership as a verified address represented by numbers and letters. The ownership address is not anonymous, but it is pseudonymous. Blockchain ledgers do not identify the actual

owner of an item of virtual currency. This opacity, combined with the ease with which someone can transfer virtual currency across borders, makes it attractive for money-laundering and other illicit activities.

Why is your customer dealing in Bitcoin?

Financial institutions should ask their customers why they want to accept Bitcoin or other virtual currencies as payment – and then verify their response. Virtual currency is risky and has the potential to mask illicit activity, facilitate money laundering, and be used to fund illegal conduct. But it can also be a legitimate payment system for your existing or potential customers. Retail businesses may want to accept Bitcoin because of the potential for greater security, lower transaction fees, brand reputation, allegiance, and growth, and PR opportunities. For Know Your Customer ("KYC") purposes, a customer who runs a PR campaign about how it will now accept payment in Bitcoin (along with cash and credit cards) may trigger one level of follow-up investigation. A customer who, during an audit, is found to have an undisclosed digital wallet will merit a heightened level of scrutiny.

Using approved wallets and exchanges.

A customer will need a digital wallet or wallets to store its digital keys, which provide access to bitcoins. They must also affiliate with an exchange to transfer bitcoins into fiat currency and vice versa. Some digital-wallet and exchange companies have more robust levels of identity verification based on transaction velocity and size. These companies can serve a pivotal role in identifying and mitigating illegal activity. Financial institutions must consider vetting and approving the digital wallets and exchanges used by customers. At a minimum, financial institutions should avoid customers associated with companies designed to make money laundering easier. One example is Dark Wallet, a digital wallet service that openly advertises its ability to make bitcoin transactions untraceable.

Which Virtual Currency Businesses are MSBs?

In 2013, FinCEN issued its initial virtual currency guidance which identified three types of virtual currency participants: "users," "exchangers," and "administrators." An exchanger is "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." Coinbase is an example of an exchanger. An administrator is "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." If a business operates as an exchanger or administrator – and this includes a virtual currency ATM operator or a payment processor – then it must register as an MSB and comply with FinCEN regulations. An MSB is heavily regulated at the federal level and must have a robust AML program suitable for its level of risk.

Virtual currency "users" who are not also exchangers or administrators need not register as MSBs. Neither do manufacturers of virtual currency ATMs. Providers of virtual wallet services need not register as MSBs unless they combine the virtual wallet services with other series that make them exchangers or administrators.

MSBs not only have to comply with federal laws requiring FinCEN registration, but also must comply with state laws requiring registration and regulation of money transmitters. Almost all states attempt to reach regulate MSBs who deal with customers in their states even though the MSB has no place of business in that state. And it is a *federal crime* not to register under an applicable state money transmittal statute.

Some states, such as North Carolina, have directly addressed virtual currencies in their money transmittal statutes. Others, such as New York and Connecticut, have created entirely new licensing schemes for virtual currency, and are in a regulatory boxing match with the Office of Comptroller of the Currency (OCC) over its recent decision to charter specialized national banks as "fintech" operations covering virtual currency MSBs.

Establishing BSA/AML/CIP/OFAC Compliance Programs for Banks Offering Services to Virtual Currency MSBs

Because a virtual currency business is inherently risky, each of the AML programs – at the bank and the MSB level – will require "enhanced due diligence." If a depository institution provides banking services to a virtual currency MSB, it must establish a robust compliance system to address its AML and related obligations. It must consider these obligations at two levels – the level of its own obligations, **and** the level of the MSB's obligations, considering the complexities that arise with virtual currency transactions.

A financial institution should decide to bank virtual currency businesses only with board approval and after extensive board review of the risks involved and the proposed procedures for addressing those risks.

Financial institutions that bank virtual currency businesses will need a BSA/AML compliance officer that understands the virtual currency ecosystem. They may even need a dedicated officer for the virtual currency part of their BSA/AML programs.

At the bank level, the "Customer Identification Program" (CIP) and "Know-Your-Customer" ("KYC") components of AML compliance will include identification of the virtual currency MSB and confirmation of its licensing with MSB regulators. The bank would need to understand the products and services the virtual currency MSB offers, the locations and markets it serves, and the anticipated volume of its activity. The bank's understanding of the MSB would need to be exceptionally thorough, and its account agreements should afford the bank extensive review and audit rights. The bank's monitoring and review of MSB accounts often might be more frequent than its review of other accounts.

The bank also must thoroughly understand how the MSB handles its own AML obligations with its customers. Technically, an MSB does not have CIP obligations, but an MSB still must have a robust AML program designed to prevent the MSB from being used to facilitate money laundering or to finance terrorist activities. Therefore, most MSBs have a *de facto* CIP program as part of their AML procedures.

A bank that offers services to MSBs must thoroughly understand the MSB's product risk, customer risk, geographic risk, and operational risk. It must review and monitor the policies and procedures adopted by the MSB to address these risks and whether these steps are likely to be effective. For example:

- Most virtual currency exchangers operate electronically. Is the bank satisfied that its KYC procedures are effective?
- Virtual currency ATMs capture KYC information at the machine. The bank needs a thorough understanding of those procedures.
- If a virtual currency payment processor services commercial accounts, does it inquire into the merchant's motivation for accepting virtual currency? Does it determine whether the merchant has lost the ability to process credit or debit card transactions, which would be a red flag to investigate further?
- Does the virtual currency business have an automated review process to flag suspicious transactions, and does the bank understand the guidelines set for suspicious transactions?
- How has the company addressed the Office of Foreign Assets Control ("OFAC") compliance, as it is very difficult to know to whom a virtual currency transaction is being sent? OFAC publishes virtual wallet numbers associated with "Specially Designated Nationals and Blocked Persons" ("SDNs"), and a virtual

currency business must have systems in place to avoid transferring virtual currency to the virtual wallet of an SDN.

Conclusion

Virtual currency has the potential to provide fast, low-cost, and secure payment transactions for customers. But given the pseudonymous nature of virtual currency transactions on the blockchain, the potential for money laundering and illegality is heightened. Many financial institutions probably will conclude that the BSA/AML risks are too high and refuse to bank MSBs involved in virtual currency – just as many depository institutions have "de-risked" traditional MSBs. Despite the high-risk, there are legitimate uses for virtual currency and legitimate virtual currency businesses. Financial institutions that bank these businesses must engage in detailed planning and incur up-front costs.

--