To Our Clients and Friends:

On November 18, 2013, the U.S. Senate Committee on Homeland Security and Governmental Affairs held a hearing on the potential risks of virtual currencies.[1] The Committee heard testimony from Jennifer Shasky Calvery, Director of the Financial Crimes Enforcement Network ("FinCEN"), Mythili Raman, Acting Assistant Attorney General of the U.S. Department of Justice ("DOJ") Criminal Division, and Edward Lowery III, Special Agent in Charge of the U.S. Secret Service Criminal Investigative Division.

Each witness emphasized the attributes of virtual currencies that are particularly attractive to criminal or terrorist organizations. The U.S. Department of the Treasury currently already subjects virtual currency administrators and exchangers to the anti-money laundering ("AML") and counter-terrorist financing ("CFT") regulatory regime established by the Bank Secrecy Act ("BSA"). Virtual currency administrators and exchangers who are U.S. persons must also comply with Office of Foreign Assets Control ("OFAC") prohibitions on transacting with Specially Designated Nationals or Blocked Persons ("SDNs").

Nonetheless, regulators remain concerned by virtual currency's potential for misuse. Financial institutions that do business with virtual currency administrators and exchangers must be attentive to these risks and should adopt precautionary procedures commensurate with those risks.

Virtual Currency and Its Abuse

According to Calvery, virtual currency is "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real money."[2] Virtual currency does not have legal tender status, but "convertible virtual currency" can be exchanged for real currency that does. Virtual currencies can be either centralized or decentralized. Centralized virtual currencies have a centralized repository and a single administrator; decentralized virtual currencies have neither.

Centralized and decentralized virtual currencies share certain attributes that make them an attractive means of exchange for illicit actors. In the Congressional testimony, each government witness called attention to virtual currency's capacity to facilitate international transfers of value between relatively anonymous users, unconstrained by transaction limits.

It is not surprising, then, that both centralized and decentralized virtual currencies have proven susceptible to abuse. Earlier this year, DOJ indicted the centralized virtual currency administrator Liberty Reserve and its executives for running a $6 billion money laundering operation that served
organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography. DOJ has also recently moved against Silk Road, an online narcotics and contraband marketplace that required its customers to pay using Bitcoin -- a popular decentralized virtual currency.

**Regulatory Measures**

The BSA is the United States' primary AML and CFT regulatory regime. It requires that "money services businesses" ("MSBs") register with FinCEN, comply with various recordkeeping rules, establish and maintain AML programs, and file currency transaction and suspicious activity reports.[3] On July 21, 2011, FinCEN published a final rule that revised the definition of an MSB to require virtual currency administrators and exchangers to comply with the BSA's registration, recordkeeping, and reporting requirements.[4]

Under FinCEN regulations, a person or entity is an MSB if it is a "money transmitter." A money transmitter is a "person that provides money transmission services," with money transmission services defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[5]

In a guidance document released on March 18, 2013,[6] FinCEN sought to clarify what types of conduct would turn a handler of virtual currency into an MSB subject to the BSA regulatory regime. The FinCEN guidance divided the virtual currency community into three categories: administrators, exchangers, and users. Administrators and exchangers are MSBs, but users are not:

- **Administrators** are persons engaged as a business in issuing a virtual currency, and who have the authority to redeem such virtual currency. The administrator of a centralized virtual currency repository that facilitates transfers of value between persons or locations is an MSB.

- **Exchangers** of virtual currency are persons engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. Importantly for financial institutions that might maintain accounts with such individuals, a person who accepts real currency from another, exchanges it into virtual currency, and credits its value to that other person's virtual currency account is an exchanger, a money transmitter and, therefore, an MSB.

- **Users** of virtual currency are persons who use convertible virtual currency to purchase real or virtual goods or services. According to FinCEN, such activity does not fit within the definition of money transmission services -- possibly because it falls within the definition's exclusion for people who "transmit[] funds only integral to the sale of goods or the provision of services."[7]

These rules and the guidance interpreting them apply to foreign and domestic MSBs alike. FinCEN sought to make sure that its regulations apply to MSBs -- like Liberty Reserve, which was based out of Costa Rica -- that are located outside of the United States but engage in money transmission services within the country. MSBs, "wherever located doing business...wholly or in substantial part within the United States," are subject to the requirements of the BSA.[8]
Doing Business with Virtual Currency Administrators and Exchangers

Even though virtual currency administrators and exchangers are now subject to the registration, recordkeeping, and reporting requirements of the BSA, financial institutions and financial services businesses that do business with them must continue to carefully assess virtual currency's vulnerability to illicit use. In previous guidance, regulators have highlighted the risks associated with entities similar to virtual currency administrators and exchangers. The recent Congressional testimony confirms that the U.S. Government views virtual currency as a source of substantial AML, CFT, and OFAC risk.

Virtual Currency Administrators and Exchangers as MSBs:

Regulators have previously cautioned financial institutions about the AML and CFT risks associated with non-bank financial institutions like MSBs. In its Bank Secrecy Act/Anti-Money Laundering Examination Manual, the Federal Financial Institution Examination Council ("FFIEC") explained that, in certain circumstances, banks that deal with MSBs "may be exposed to a higher risk for potential money laundering activities."[9] It requires banks to assess the risks of a particular MSB customer and perform due diligence that is proportional to the level of risk it assigns.

Virtual currency administrators and exchangers may prove to be risky customers. In her Congressional testimony, Calvery emphasized some particularly problematic attributes of virtual currency -- it allows its users to remain relatively anonymous, is accessible all over the world, allows for international transactions, and does not typically have transaction limits. Each of these attributes has been previously identified by FFIEC, FinCEN, or both as an indicator of heightened AML and CFT risk.[10]

At minimum, the FFIEC requires banks opening and maintaining accounts for MSB customers to apply the BSA-mandated Customer Identification Programs, confirm the customer's compliance with FinCEN and state registration requirements, ascertain whether the customer is an agent of another MSB, and conduct a basic BSA/AML risk assessment. When dealing with riskier customers like virtual currency administrators and exchangers, additional investigation may be necessary. The FFIEC does not require any specific steps, but suggests that a review of the customer's BSA/AML program may be appropriate. It also recommends reviewing a list of the customer's agents, both within and outside the United States.

Virtual Currency Administrators as Third-Party Payment Processors:

Another potential source of concern for regulators is the similarity between virtual currency administrators and third-party payment processors. Third-party payment processors contract with merchants to process transactions between the merchant and its customers. Many accomplish this with the use of bank accounts. Because the processor's bank has no direct relationship with its merchants, the "bank is unable to identify and understand the nature and source of the transactions processed" through the account.[11] As a result, third-party payment processors may be an attractive option for higher-risk merchants who would prefer not to deal directly with a bank.
Third-party payment processors can cause especially acute problems in the OFAC context. OFAC regulations require banks to block the accounts of and prohibit unlicensed trade or financial transactions with specified countries, entities, and individuals.\[12\] OFAC maintains a list of these SDNs and recommends that new accounts be compared with its list prior to being opened, or shortly thereafter. Financial institutions should also review transactions with the aid of available technology to make sure that no parties to the transaction are SDNs. Knowing the identity of the parties to a particular account or transaction is obviously essential to this process.

The Government considers that third-party payment processors can undercut the OFAC screening process by keeping financial institutions in the dark about the nature of and parties to the transactions being processed through their accounts. Virtual currencies pose analogous challenges. According to the Congressional testimony of Special Agent in Charge Lowery, criminals prefer to use digital currency because it offers "[t]he greatest degree of anonymity for both users and transactions."\[13\] Virtual currency administrators might contract with "higher-risk merchants" and effectively shield them from direct contact with the bank. Without an opportunity to check OFAC lists for the parties to the administrator's underlying transactions, the financial institution servicing the account runs the risk that the administrator's merchants are actually SDNs.

The FFIEC advises that, at a minimum, a bank doing business with a third-party processor should "authenticate the processor's business operations and assess their risk level."\[14\] In other words, banks must learn as much about the processor and its merchants as possible. Banks should consider requiring the processor to identify its major merchants and verify that they are operating legitimate businesses. They might also review a processor's due diligence standards for new merchants. Given the similarity between third-party processors and virtual currency administrators, banks servicing administrator accounts should take the same steps.

**Conclusion**

Virtual currency administrators and exchangers are now subject to both the BSA and OFAC regulation. Nonetheless, through their recent Congressional testimony, federal regulators have signaled that they continue to view virtual currency as a substantial source of AML, CFT, and OFAC risk. Their current view is supported by previous guidance, which has warned about the risks inherent in doing business with entities like virtual currency administrators and exchangers, which allow for international transfers of value between relatively anonymous users, unconstrained by transaction limits. Banks may still elect to do business with virtual currency administrators and exchangers. Effective compliance with the BSA and OFAC regulations, however, requires those who do so to take additional precautions.


[3] See 31 C.F.R. § 1022.380 (2012) (creating registration requirements); id. at § 1022.210 (creating requirement to establish and maintain an anti-money laundering program); id. at § 1010.311 (creating requirement to file currency transaction reports); id. at § 1022.320 (creating requirement to file suspicious activity reports).


[8] Id. at § 1010.100(ff). There is an exclusion, however, for foreign banks. Id. at § 1010(ff) (8)(i).


[10] See, e.g., id. at 310 -- 11 (explaining that MSBs are less risky when they limit their money-transmitting activities to domestic entities and low-dollar amounts).

[11] Id. at 239.

[12] Id. at 148.


Gibson, Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, any of the following lawyers, or any member of the firm's International Trade Regulation and Compliance Practice Group or Financial Institutions Practice Group.

Judith A. Lee - Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Arthur S. Long - New York (+1 212-351-2426, along@gibsondunn.com)
Amy G. Rudnick - Washington, D.C. (+1 202-955-8210, arudnick@gibsondunn.com)
Marcellus A. McRae - Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Andrea Farr - Washington, D.C. (+1 202-955-8680, afarr@gibsondunn.com)
Michael Willes - Los Angeles (+1 213-229-7094, mwilles@gibsondunn.com)

© 2014 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.