

## Virtual Currencies in the Crosshairs

BY GORDON GRIFFIN

On May 28, 2013, Liberty Reserve, a self-described virtual currency provider, was designated by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) as a primary money laundering concern, and the Department of Justice simultaneously indicted several of its officers. The indictments and the FinCEN finding read like a movie script, complete with a shadowy network of hackers, drug dealers, and international criminals relocating to a nonextradition country to protect their money laundering operation. The government's allegations describe an enterprise responsible for laundering billions of dollars over a period of years through the use of Liberty Reserve's virtual currency—the "LR."

So what is a virtual currency, and how does it lend itself to criminal activity? While there is no universally accepted definition, FinCEN describes a virtual currency as a medium of exchange that is not legal tender in any jurisdiction. This definition highlights one of the difficulties regulators face when addressing virtual currencies and one of the reasons that would-be money launderers might find a virtual currency attractive: the lack of a government issuer or regulator responsible for tracking and managing the currency. The story of Liberty Reserve provides insight into both how virtual currencies work, as well as how they can be exploited for criminal gain.

### Digital Equivalent of a Cash Transaction

Liberty Reserve was arguably designed to provide its customers with anonymity. According to the indictment and FinCEN's finding, Liberty Reserve provided accounts to its customers without requiring any sort of name verification. One account was listed under the name "Russia Hackers," and an undercover government agent was able to obtain an account under the name "Joe Bogus." This "no questions asked" policy made Liberty Reserve an attractive venue for money launderers and other criminals.

Money could not be deposited directly into Liberty Reserve accounts. Instead, a depositor would

have to purchase LRs from an exchanger, some of which were owned by the owners of Liberty Reserve, and most of which operated in countries with few anti-money laundering (AML) controls. These exchangers would charge high fees, both to convert currency into LRs, and then to convert the LRs back into real currency. For its part, Liberty Reserve charged approximately 1 percent per transaction.

Once an individual had LRs in his or her account, he or she could transfer between accounts with only a transaction number linking the two accounts, and even these could be erased if you were willing to pay a small fee. Users had enough trust in the system that they were willing to accept LRs as payment for goods or services.

While there were almost certainly some legitimate business interests with accounts at Liberty Reserve, the indictments allege that the overwhelming majority of the account holders were involved in a criminal enterprise. Other virtual currencies appear to have more legitimate clientele, but there are risks for legitimate businesses using virtual currencies. Next, we'll explore how to examine and mitigate some of those risks for participants in virtual currency markets.

### To Use or Not to Use Virtual Currencies?

First, examine your needs and activities involving virtual currencies. What type of transactions will you be conducting? For the purposes of AML responsibilities, the threshold question is whether or not you will be considered a money services business (MSB). FinCEN issued a guidance on March 18, 2013, applying its definition of MSBs under the Bank Secrecy Act (BSA) to virtual currency. This guidance describes three classes of participants in virtual currency arrangements and their respective obligations as MSBs.

As defined by FinCEN's guidance, a *user* of virtual currency is just that, anyone who "obtains virtual currency to purchase goods or services." (FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 2 (2013), available at <http://tinyurl.com/lcm3e7>.) Users of virtual currency are not MSBs under FinCEN regulations. Accordingly, users are not subject to the registration, reporting, AML compliance program, and recordkeeping obligations that FinCEN maintains for MSBs.

The next two categories of virtual currency participants are *administrators* and *exchangers*. As per FinCEN's guidance, an exchanger is "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency," while an administrator is "a person engaged as a business in issuing (putting into circulation) a virtual currency, and



**GORDON GRIFFIN** is an associate in the Government Contracts Group in the Washington, D.C., office of Crowell & Moring.

who has the authority to redeem (to withdraw from circulation) such virtual currency.” (*Id.*) An exchanger or an administrator that accepts and transmits a virtual currency or buys or sells virtual currency is a money transmitter under FinCEN regulations, and an MSB. It is important to note that, unlike other types of MSBs, money transmitters have no activity threshold to be subject to all of the regulations for MSBs; if you’re a money transmitter, you’re an MSB, regardless of the amount of money transmission activity.

MSBs are required to have effective AML programs that are reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The programs must adequately address the risks inherent in the business, and must (1) incorporate written policies, procedures, and internal controls reasonably designed to assure compliance with the BSA; (2) designate a compliance officer responsible for day-to-day compliance with the BSA; (3) provide education and/or training of appropriate personnel; and (4) provide for independent review to monitor and maintain an adequate program. (31 C.F.R. § 103.125.)

### Future of Virtual Currency and Decentralization

The government has been able to target both the individuals involved with Liberty Reserve as well as the institution itself to prosecute AML violations precisely because of its centralized nature: Liberty Reserve had administrators, employees, and even a place of business. So what happens when you remove all of the centralized structure around a virtual currency? Bitcoin and other similar decentralized virtual currencies happen. Bitcoin is an open-source “peer-to-peer” digital currency that has no administrator. Rather, it uses an algorithm that constantly checks itself against other Bitcoin users to verify its amounts and locations.

The March 18, 2013, FinCEN guidance on virtual currencies acknowledged this difference. It described a decentralized virtual currency as one that has no administrator or central repository, and that persons may obtain through their own computing or manufacturing effort. Users of this type

of virtual currency are not MSBs. This leaves only one category of persons open to FinCEN and law enforcement scrutiny: exchangers. Bitcoins can be purchased with “real” currencies, and several companies exist to serve just that purpose. This is the only point in the current Bitcoin model that lends itself to regulatory enforcement.

Bitcoin currently appears to be more attractive to speculators than to consumers and consumer businesses, due to the large fluctuations in its value. One notable exception is illicit websites. For example, in 2011, Senators Charles Schumer (D-NY) and Joe (D-WV) wrote a letter to Attorney General Eric Holder asking him to take action against the website Silk Road, where, according to the letter, one can purchase illegal drugs and weapons, and the only accepted currency is the Bitcoin. But as Bitcoin acceptance becomes more ubiquitous, and the fluctuations in value level out, the need for money exchangers will fall in line more with national currencies. This may very well lead to difficulties for regulators at FinCEN and the Department of Justice. It is not difficult to imagine a future in which a transfer of Bitcoins between two individuals valued at \$100,000 could be commonplace. Bitcoin transactions are untraceable, they do not involve any financial institutions, and they effectively sidestep any regulatory enforcement mechanism currently in place.

While Bitcoin users may be seeking anonymity, it is clear that the global regulatory trend, spearheaded by groups like the Financial Action Task Force (FATF), is calling for greater transparency. FinCEN’s director noted in a recent speech that the agency is not looking to prohibit virtual currencies, but one would expect that, if virtual currencies are to gain ground among traditional merchants and consumers, they will have to submit to some minimum AML controls.

Technology and innovation may have outpaced the law, but it seems clear from the Liberty Reserve investigation that this is an area that law enforcement will be paying attention to in the future. Expect more to come from Treasury and FinCEN, as well as input from other government agencies, on the rules surrounding virtual currencies. ■