New York Law Journal

September 30, 2013

Uncertainty Looms for Digital Currency Providers and Regulators

by Laura Colombell Marshall and Shawn Patrick Regan

Since the indictment of digital currency provider Liberty Reserve, new questions have been raised about what, if anything, that prosecution may portend for a growing population of digital currency providers and the law enforcement and regulatory communities. In May 2013, Liberty Reserve was indicted for conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business and operation of an unlicensed money transmitting business.[1] The indictment has been characterized as the largest money laundering prosecution in history and an "important *step* towards reining in the Wild West of illicit Internet banking."[2]Specifically, Liberty Reserve is alleged to have processed 55 million transactions and laundered $6 billion in criminal proceeds since 2006.[3] In addition to criminal charges, a civil forfeiture complaint and restraining order were filed against 35 domain names associated with pre-approved third-party exchangers recommended by Liberty Reserve on its website.[4]

Simultaneous with the federal indictment, the Financial Crimes Enforcement Network (FinCEN) announced the designation of Liberty Reserve as a "financial institution of primary money laundering concern" under the Patriot Act.[5] The coordinated action evidences a policy of pursuing rogue digital currencies through orchestrated criminal, civil and regulatory means. It may also signal an increase in the level of scrutiny applied to financial institutions providing services to the digital currency industry.

In its simplest form, digital currency is an electronic currency that exists on the Internet and is characterized by the absence of a centralized bank.[6] A digital currency administrator like Liberty Reserve operates by allowing users to open accounts on its website. In contrast to a legitimate financial institution, the user's identifying information is not verified, which serves to provide the first layer of anonymity to the account holder. In addition, digital currency users cannot fund their accounts by direct transfers of money or credit card payments. Rather, the user can make deposits or withdrawals into the account only through a third-party exchanger.

The exchangers buy and sell digital currency from the administrator in bulk. This allows the exchanger to transact with a particular user, receiving payments and in turn issuing credit to the user's account for a processing fee. Once the credit of digital currency is in the user's account, the user can directly transact with other users for goods and services, or transfer funds without the exchange of goods by way of an exchanger on either side of the transfer. The end result is that the transactions and transfers happen with complete anonymity and without the paper trail that would have been created through the traditional banking system.[7]

A series of important milestones predated the Liberty Reserve indictment and provide meaningful insight to the future of increased regulatory enforcement. In 2007, the first digital currency provider was indicted for operating an unlicensed money services business (MSB). In *United States v. e-gold*, the government indicted the digital currency provider, a primary exchanger and individual operators of both. The defendants challenged the indictment on the grounds that they did not meet the definition of an MSB because they never engaged in the physical transfer of currency.[8] Although the district court rejected the argument and the defendants later pleaded guilty, the case highlighted the reality that the statutes and regulatory framework at that time were ambiguous in terms of the application to digital currencies. As a result, digital currencies were able to hide behind the vagueness, and operate free from any restrictions at all.

In July 2011, FinCEN published a final rule substantially revising the definition of a money transmitter.[9] Specifically, the definition was expanded to apply to 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."[10] In addition, the definition was revised to include entities doing business as a transmitter, "whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part in the United States…."[11] The new MSB rule was thus drafted with some foresight and in recognition of the fact that payment processors were evolving and moving towards technology-based methods to service customers. Notwithstanding the obvious implications of the new MSB rule, FinCEN did not issue specific guidance on the application of BSA regulations to digital currencies until March 2013. Two months before the Liberty Reserve indictment was announced, FinCEN issued Guidance affirmatively stating that an "administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter…."[12]

The Liberty Reserve case remains pending and it remains to be seen whether the regulatory changes and guidance issued since *United States v. e-gold* will be enough to stave off anticipated challenges to the indictment of a digital currency provider largely operating online and beyond U.S. borders. The allegations in the indictment make clear, however, that the basis for jurisdiction is grounded in the number of users in the United States and the transfer of funds through at least one correspondent bank in New York. The indictment alleges that Liberty Reserve touted itself as serving millions around the world including the United States, but at no time registered with the U.S. Department of Treasury (FinCEN).[13] The indictment also details the founding of Liberty Reserve in a manner to evade U.S. law enforcement and regulators by incorporating in Costa Rica, and using exchangers primarily in Malaysia, Russia, Nigeria and Vietnam.[14] The indictment further alleges that an estimated 200,000 users were located in the United States;[15] however, there are no specific allegations that users in the United States engaged in the criminal acts listed as predicates for the money laundering conspiracy.

With respect to the conspiracy to operate an unlicensed money transmitting business, the indictment specifically references the newly broadened definition of MSBs as applying to foreign-based businesses.[16] The single overt act listed is a wire transfer in November 2011 from a bank in Costa Rica to an account in Cyprus, through a correspondent bank account in New York.[17] In sum, the allegations in the indictment are based in large part on activity occurring outside the United States. The prosecution is seemingly indicative of how aggressively the

Department of Justice will pursue illicit digital currencies, and the extent to which the United States is cooperating with the global law enforcement community and vice versa.

In coordination with the prosecution, FinCEN designated Liberty Reserve as a "primary money laundering concern" under §311 of the Patriot Act, marking the first use of the special measure in relation to a digital currency.[18]The action essentially triggers AML-compliance requirements under the BSA for domestic financial institutions, to include extensive record-keeping and prohibitions on the maintenance and opening of correspondent accounts for use by the designated concern.[19]

This concerted action suggests that the focus going forward may well expand beyond the digital currencies themselves, to domestic financial institutions that deal, even indirectly, with administrators or exchangers of digital currency. The requirement that banks apply heightened scrutiny to third-party payment processors is not a new concept. Third-party payment processors are generally viewed as non-bank entities in the business of processing financial transactions for clients that do not have a relationship with the processor's bank. Regulators have repeatedly warned of the increased potential for money laundering occasioned by third-party processors and specifically MSBs.[20]

In October 2012, FinCEN issued guidance to banks for filing Suspicious Activity Reports (SARs) on accountholders acting as third-party payment processors.[21] Although the guidance did not associate the risks presented by third-party payment processors with digital currency per se, financial institutions were advised to determine whether the processors "have obtained all necessary state licenses, registrations, and approvals."[22] One month later, an enforcement action led by FDIC and FinCEN was announced against the First Bank of Delaware for its dealings with third-party payment processor customers.[23] The bank was fined $15 million for failure to implement an effective BSA/AML compliance program. Specifically, the bank was faulted for accepting third-party payment processors as customers without assessing the inherent AML risks, and not performing certain actions including actual site visits.[24] There is a widely held belief in the financial services industry that the rules and guidance issued with respect to MSBs resulted in banks systematically closing accounts for these customers to avoid compliance pitfalls.

These circumstances raise concerns about the present expectations for financial institutions in terms of dealing with digital currencies in light of specific guidance from FinCEN applying BSA regulations to administrators and exchangers. Transactions between the exchanger and the administrator of a given currency occur online. By design, transfers of digital currency between the two entities occur *outside* traditional banking channels. As such, financial institutions cannot possibly know what they cannot see. The question becomes how will institutions apply existing regulations to the digital currency industry given the technology-based nature of the transactions and, more importantly, what enforcement actions might follow for perceived AML failures in banking digital currency customers.

In addition to the extension of federal requirements, another implication of the prosecution will likely be increased regulation by the states based on state licensing requirements for MSBs. Leading that effort, the New York State Department of Financial Services (DFS) recently "launched an inquiry into the appropriate regulatory guidelines that it should put in place for

virtual currencies" and made "requests for information from virtual currency firms."[25]Reports indicate that DFS has issued 22 subpoenas to money transmitters, exchangers, digital currency providers and their investors requesting information that could be used to create state regulations specifically tailored to the unique nature of digital currency.

The Senate subcommittee on homeland security is conducting an inquiry of its own in response to concerns from law enforcement about the industry and in light of a pending application with the SEC to allow institutional investors to begin trading digital currency.[26] This could result in legislation designed to prevent use of digital currency by criminals, while still allowing it to emerge as a mainstream payment method for goods and services.

Optimists in the wake of Liberty Reserve think that digital currency businesses will move to implement BSA/AML compliance programs and follow applicable U.S. laws and regulations. While some businesses will fall in line to continue the growth of digital currency in legitimate markets, others have and will move in the opposite direction and possibly restrict access for users located within the United States. If the Liberty Reserve case and recent FinCEN guidance has its desired effect, at least the potential exists for financial institutions to seek new lines of business with compliant digital currencies and perhaps even regard them as "desirable and profitable customers."[27] For this to happen, however, regulators will need to proceed with restraint and resist imposing unrealistic standards for managing risks in what is still unchartered territory for most financial institutions.

Laura Colombell Marshall, *a partner at Hunton & Williams in Washington, D.C., and Richmond, Va., practices in the white-collar crime and internal investigations groups.* **Shawn Patrick Regan**, *a partner in New York, practices in the securities litigation and SEC enforcement group, as well as the white-collar crime group.*

Endnotes:

1. 18 U.S.C. §§1956(h), 371 and 1960.

2. Liberty Reserve Press Conference, Prepared Remarks of U.S. Attorney Preet Bharara, May 28, 2013 (emphasis added).

3. *United States v. Liberty Reserve*, 13CRIM368 (S.D.N.Y.); Indictment at 5.

4. *United States v. WM-Center.com*, 13CIV3565 (S.D.N.Y.).

5. See Liberty Reserve Press Release, United States Attorney's Office (S.D.N.Y.), May 28, 2013, available at http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php; see also 31 U.S.C. §5318A.

6. Not all digital currencies operate in the same way and will vary in terms of what drives the value of the currency. For example, value for the largest digital currency provider, Bitcoin, is derived from a process called "mining" where individuals utilize Bitcoin software to generate the coins.

7. For an additional fee, Liberty Reserve offered users the option of hiding their Liberty Reserve account number notwithstanding the "already opaque system." *United States v. Liberty Reserve*, 13CRIM368 (S.D.N.Y.); Indictment at 7.

8. 550 F. Supp. 2d 82, 88 (DDC 2008).

9. 76 Fed. Reg. 43,585 (July 21, 2011).

10. 31 C.F.R. §1010.100(ff)(5)(i)(A).

11. Id.

12. FinCEN Guidance, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013). The guidance addresses "convertible virtual currency" which is largely interchangeable with the term "digital currency." The FinCEN guidance was intended to apply to a "medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." Id. at 1.

13. *United States v. Liberty Reserve*, 13CRIM368 (S.D.N.Y.), Indictment at p. 2.

14. Id. at 6 and 9.

15. Id. at 4.

16. Id. at 17.

17. Id. at 19.

18. 31 U.S.C. §5318A(c).

19. 31 U.S.C. §5318A(b).

20. FinCEN Advisory, "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States" (April 26, 2005).

21. FinCEN Guidance, FIN-2012-A010, Risk Associated with Third-Party Payment Processors (Oct. 12, 2012).

22. Id. (citing FinCEN, "Advisory—Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States," (April 26, 2005).)

23. In the Matter of: First Bank of Delaware, Matter No. 2012-01, Assessment of Civil Penalty (Nov. 19, 2012).

24. Id. at 4.

25. Memo Re: Notice of Inquiry on Virtual Currencies, Benjamin M. Lawsky, Superintendent of Financial Services (Aug. 12, 2013).

26. Letter to Homeland Security Secretary Napolitano on Virtual Currencies (Aug. 13, 2013), available at http://www.hsgac.senate.gov/reports/letters.

27. Prepared Remarks of FinCEN Director Jennifer Shasky Calvery, "The Virtual Economy: Potential, Perplexities and Promises," at the United States Institute of Peace (June 13, 2013).