Bloomberg BNA

BNA's Banking Report™

ELECTRONIC COMMERCE

Bitcoin, Banks & Billions: Regulatory and Compliance Implications of Bitcoin-Based Consumer Banking



By Elizabeth McGinn, Sasha Leonhardt and Sara Ruvic

"The global enforcement action we announce today is an important step toward reining in the 'Wild West' of illicit Internet banking."

Preet Bharara, U.S. Attorney, SDNY

Elizabeth McGinn is a partner, and Sasha Leonhardt and Sara Ruvic are attorneys, in the Washington, DC office of BuckleySandler LLP. They advise clients on consumer financial services, e-commerce, and privacy-related issues. They may be reached at emcginn@buckleysandler.com, sleonhardt@buckleysandler.com, and sruvic@buckleysandler.com, respectively.

Earlier this year, the U.S. Attorney for the Southern District of New York, Preet Bharara, made headlines for bringing the largest online money laundering case ever.[1] Over a span of seven years, Liberty Reserve—a Costa Rican company started by an American expat—allegedly laundered billions of dollars worldwide, including transactions involving 200,000 customers in the United States.[2] Bharara, using the authority provided in Section 311 of the Patriot Act, seized Liberty Reserve's domain name and restricted activities for 45 different Liberty Reserve accounts.

On Sept. 30, Bharara's office took action against a second virtual commerce platform—Silk Road—which allegedly provided an anonymous platform to buy and sell drugs, forged documents, counterfeit currency, stolen identity documents, anonymous bank accounts, firearms, and even arrange contracts with hitmen.[3] To ensure anonymity, Silk Road only permitted transac-

[1] Marc Santora, William K. Rashbaum & Nicle Perlroth, *Firm Accused in Laundering of $6 Billion*, N.Y. Times, May 28, 2013, at A1.

[2] *Id.*

[3] Sealed Post-Complaint Protective Order Pursuant to 18 U.S.C. § 983(j)(l), United States v. Ulbricht, No. 13-CIV.6919, at 10-11 (S.D.N.Y. Sept. 30, 2013).

 ISSN 0891-0634

tions in a new virtual currency known as ''Bitcoin.''[4] Before this civil forfeiture action and the arrest of Silk Road's creator, Silk Road was estimated to have generated $1.2 billion in illicit sales and $80 million in commissions for its founder—all in untraceable, electronic Bitcoins.[5]

Having taken criminal action against a virtual currency, Liberty Reserve, and an electronic commerce platform specializing in Bitcoin transactions, Bitcoins themselves are all but certain to be an emerging area of focus for the Department of Justice (''DOJ''). In the past few years, Bitcoin has been considered the most promising of several different virtual currencies. Bitcoin has received accolades large and small—publications as varied as *Forbes*, *Bloomberg*, the *New York Times*, the *Wall Street Journal*, *Businessweek* and *Wired* have dedicated precious space to Bitcoin. Many Europeans, wary of volatile national currencies and unstable fiscal policy, are shifting their own savings into government-neutral Bitcoins.[6] The Winklevoss twins of Facebook fame have put their faith in Bitcoin, proclaiming, ''This isn't a bubble or tulip mania,''[7] and ''It's gold 2.0.''[8] They backed up their words by exchanging a substantial portion of their own money for the virtual currency, and they currently own one percent of the world's Bitcoins.[9] Even the extortionist who threatened to release former presidential candidate Mitt Romney's tax returns demanded payment only in Bitcoins.[10]

With virtual currencies becoming a fixture of the global economy, it is critical that financial institutions understand these 21st century monetary tools. And, of all the virtual currencies emerging in the dynamic area of e-commerce, none more perfectly demonstrates the technical, regulatory and legal challenges facing financial institutions than Bitcoin.

What is Bitcoin?

Created in 2009, Bitcoin is the brainchild of Satoshi Nakamoto[11] and is a virtual currency designed to build upon—and improve upon—existing Internet commerce by combining the best elements of both a currency and a payment system. Like currency, Bitcoins can be transferred from one person to another or exchanged for dollars, euros, yen or any other traditional, government-backed currency. Like a payment system, all of the information for a Bitcoin transfer is electronic and encrypted, thereby making Bitcoin transfers both secure and instantaneous.

Because of their dual nature, Bitcoins should not be thought of as merely a substitute for traditional currency; Bitcoins are strings of data, and Bitcoin commerce literally exchanges goods and services for these strings of data. For those businesses that do not accept Bitcoins, one can go to a Bitcoin exchange—the digital equivalent of a money changer—to trade Bitcoins for traditional currency.

Bitcoin is growing quickly in usage and it appears to be the most viable virtual currency to date. At the current exchange rate, the 11.8 million Bitcoins in circulation have an equivalent value of over $2 billion, and the exchange rate appears to be stabilizing from the wild shifts seen just a few years ago. While small in light of the global economy, the fact that a virtual currency—which has no shareholders, no formal leadership, no profits and an uncertain future—has reached a valuation of $2 billion in just four short years indicates the strong market demand for such a product.

Bitcoin's strong position in the virtual currency world comes from several systematic advantages that Nakamoto built into the currency. Unlike many competing virtual currencies, Bitcoins are ''bidirectional''—that is, users can both buy and sell Bitcoins by exchanging them for traditional currency. Most other virtual currencies are either closed (they cannot be exchanged for traditional currency or goods) or unidirectional (traditional currency can purchase virtual currency, but not vice versa). Bitcoin also has the advantage of being entirely decentralized; there is no main server or governing body that creates Bitcoin's monetary policy. Rather, Nakamoto wrote the code for Bitcoin and disappeared, with the Bitcoin network existing—and now thriving—on its own.

From Dollars to Data: Bitcoin's Advantages (and Disadvantages)

Nakamoto created Bitcoin with the goal of providing a cheap, effective alternative to central and consumer banks.[12] Accordingly, Bitcoin has grown in popularity because of several key differences with traditional banking:

- *Bitcoin transactions are anonymous*. The Bitcoin network keeps a distributed record of every Bitcoin transaction, tracked by each Bitcoin user's account number. However, there is no central database that connects the Bitcoin account number with an individual's identity, thereby making Bitcoin transactions anonymous. Furthermore, an individual can set up an unlimited number of free Bitcoin accounts; even if a single account were connected to an individual, using

[4] *Id.* at 2

[5] Sealed Verified Complaint, United States v. Ulbricht, No. 13-CIV.6919, at 4 (S.D.N.Y. Sept. 30, 2013).

[6] Ross Kenneth Urken, *Are Bitcoins Becoming Europe's New Safe Haven Currency?*, DailyFinance (Apr. 8, 2013, 2:39 PM), http://www.dailyfinance.com/2012/06/18/Bitcoins-euro-europe-safe-haven-currency.

[7] Stacy Cowley, *The Winklevoss Twins Are Bitcoin Bulls*, CNNMoney (May 19, 2013, 11:35 AM), http://money.cnn.com/2013/05/18/investing/winklevoss-Bitcoin.

[8] Maureen Farrell, *Winklevoss Twins: Bitcoins Better Than Gold*, CNNMoney (Sept. 17, 2013 12:38 PM), http://money.cnn.com/2013/09/17/investing/Bitcoin-winklevoss-twins.

[9] Stephanie Baker, *Bitcoin Bets Feed Twitter Dreams as Regulators Circle*, Bloomberg News (Oct. 2, 2013), http://www.businessweek.com/news/2013-10-02/bitcoin-led-by-winklevii-spurs-twitter-dreams-as-regulators-fret.

[10] Robert W. Wood, *Indictment in Bitcoin Bidding Scheme for Mitt Romney's Tax Returns*, Forbes (June 27, 2013 2:27 AM), http://www.forbes.com/sites/robertwood/2013/06/27/indictment-in-Bitcoin-bidding-scheme-for-mitt-romneys-tax-returns.

[11] No doubt, part of the allure of Bitcoin is that Satoshi Nakamoto is an alias—the actual creator of Bitcoin has never been identified. Nakamoto's original paper outlining Bitcoin was published in 2007, and he has made occasional online postings since, but the Nakamoto alias has been inactive since 2010. *See* Benjamin Wallace, *The Rise and Fall of Bitcoin*, Wired, Dec. 2011, at 99.

[12] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), *available at* http://Bitcoin.org/Bitcoin.pdf.

  BBR ISSN 0891-0634

multiple accounts would make Bitcoin transactions nearly impossible to track. And because Bitcoin transactions do not require a traditional bank account, it is possible to trade in Bitcoins without ever revealing one's identity.

■ *Bitcoins are (allegedly) secure*. One of Bitcoin's strengths is that security is an inherent part of the Bitcoin architecture—that is, it is impossible to separate Bitcoins from the secure system used to transfer Bitcoins. Every Bitcoin transfer employs public and private key cryptography, which is a standard systems used to protect online banking data worldwide. Furthermore, all transactions are verified and logged through Bitcoin's distributed network, thereby providing further protection for deposits.

However, this security has limits. As discussed above, Bitcoins are merely strings of data stored on a person's computer, smartphone, or other device—if a person's device is hacked, lost, or destroyed, that person could lose all of his or her Bitcoins. Unlike bank data, which is constantly archived to protect against technical failures, the Bitcoin network does not automatically back up an individual's account data, making it difficult to recover lost funds.[13] Additionally, while Bitcoins themselves may be secure, there have been several instances of hackers stealing money from online Bitcoin exchanges.[14] In September 2012, hackers stole $250,000 in Bitcoins from the virtual currency exchange Bitfloor.[15] Without sufficient funds to repay customers, Bitfloor considered declaring bankruptcy.[16] And earlier in 2012, hackers stole $90,000 from Bitcoin exchange Bitcoinica.[17]

■ *Bitcoins are cheap*. Because Bitcoin has its own payment transfer system, it has low transaction costs. Transferring Bitcoins themselves is free, and there is no requirement to pay a third party for the convenience of transferring Bitcoins electronically. There are no bank fees, credit card charges, or payment processing costs. Because Bitcoins do not require any centralized infrastructure, they may be a desirable option to those seeking to reduce transaction costs or who lack convenient access to a bank. The only Bitcoin-related costs occur when transferring Bitcoins into another currency; currently these charges are relatively small, and similar charges would be part of any currency exchange transaction.

■ *Bitcoins are independent*. For many users, Bitcoins may offer a stable source of value because they are neither backed by gold nor issued by a government. Some believe that removing dependence on a government makes Bitcoin a safer alternative to traditional currencies.[18] Rather than rely upon a central bank or treasury to speed or slow the flow of currency in an economy, Bitcoins are created—and their integrity guaranteed—by the neutral Bitcoin algorithm. Bitcoins are not injected into the system when a central bank declares it prudent; instead, Bitcoin users ''mine'' new Bitcoins by using their computers to solve increasingly-complicated mathematical problems. As more Bitcoins enter circulation, the Bitcoin algorithm slows its rate of Bitcoin production to stabilize the Bitcoin economy.

■ *Bitcoins are finite*. The Bitcoin algorithm ensures that Bitcoin remains a finite currency—that is, only the predetermined 21 million Bitcoins will ever exist. As economists struggle to make sense of the recent recession, the value of a finite currency has been fiercely debated. While some who oppose centralized banking believe the finite number of Bitcoins will stabilize the Bitcoin market by reducing uncertainty, others caution that such a limited monetary supply could lead to deflation.

■ *Bitcoins shift payment risk*. In the early days of the Internet, and even today, there was a significant amount of fraud in online commerce. Without Bitcoin, an unscrupulous buyer could agree to purchase goods from a seller via credit card, wait until the goods were received, and then cancel the credit card transaction—thereby obtaining goods free-of-charge. Financial institutions and online markets have attempted to reduce this through programs such as eBay's complaint filing database and buyer/seller rating systems. Bitcoin takes a different approach: because there is no credit card intermediary to cancel the payment, once a Bitcoin payment is made, it is irreversible. Thus, Bitcoin shifts the risk from seller to buyer and creates an Internet-age version of sending a cash payment before the seller ships the product.[19]

Lessons from Liberty Reserve

Although not tied to any central government, virtual currencies are nevertheless subject to national laws, and the *Liberty Reserve* case illustrates how the government can rein in a virtual currency. Upon finding reasonable ground to conclude that a foreign action or entity is of ''primary money laundering concern,'' Section 311 of the Patriot Act grants the Secretary of the Treasury the authority to require domestic financial institutions and agencies to take ''special measures'' to handle the ''primary money laundering concern.'' According to

[13] Although some programs have been created to automate the task of backing up a Bitcoin wallet file, a user must be savvy enough to download, install, and maintain such a program. And even this may not be enough to stop a particularly dedicated hacker or protect against a damaged or destroyed computer.

[14] *E.g.*, Robert McMillan, *Sure, You Can Steal Bitcoins. But Good Luck Laundering Them*, WIRED (Aug. 27, 2013, 6:30 AM), http://www.wired.com/wiredenterprise/2013/08/bitocoin_anonymity.

[15] Devin Coldeway, *$250,000 Worth of Bitcoins Stolen in Net Heist*, NBC NEWS (Sept. 5, 2012, 3:35 PM), http://www.nbcnews.com/technology/250-000-worth-Bitcoins-stolen-net-heist-980871.

[16] *Id.*

[17] Tim Worstall, *Another Bitcoin Theft at Bitcoinica*, FORBES (May 5, 2012, 1:01 PM), http://www.forbes.com/sites/timworstall/2012/05/15/another-Bitcoin-theft-at-bitconia.

[18] *See, e.g.*, Peter Ferrara, *The Federal Government's Reaction to Bitcoin is an Acknowledgement of the Dollar's Vulnerability*, FORBES (Aug. 25, 2013, 8:00 AM), http://www.forbes.com/sites/peterferrara/2013/08/25/the-federal-governments-reaction-to-Bitcoin-is-an-acknowledgement-of-the-dollars-vulnerability/#

[19] In creating Bitcoin, Nakamoto acknowledged that this system could replace buyer fraud with seller fraud and that a ''certain percentage of [seller] fraud is accepted as unavoidable.'' Nakamoto, *supra* note 11, at 1. However, he believed that buyer fraud was a greater problem for e-commerce, and that creating such a system would significantly lower transaction costs overall. *Id.* at 1.

the Treasury Department, Liberty Reserve was structured to ''facilitate money laundering and other criminal activity while making any legitimate use economically unreasonable.''[20] Based upon this belief and an indictment from a grand jury, the DOJ obtained an order for the forfeiture of Liberty Reserve's assets.

The *Liberty Reserve* case is the first instance in which the Patriot Act has been used against a virtual currency provider. By employing this section of the Patriot Act—and the Act's powerful seizure provision—the DOJ sent a clear message that virtual currencies are under scrutiny.

While Liberty Reserve had several elements that made it uniquely susceptible to action under the Patriot Act, only some of those high-risk elements exist in the Bitcoin universe. Like Bitcoins, Liberty Reserve had its own digital currency known as ''LR.''[21] Seeking anonymity akin to Bitcoin, individuals on the Liberty Reserve network could set up anonymous accounts with a false name and address as Liberty Reserve did not verify an individual's identity.[22] Liberty Reserve, like the Bitcoin network, did not directly handle money, instead relying upon third-party exchanges to transfer traditional currency to virtual currency.[23]

Although Bitcoin lacks a centralized infrastructure and did not engage in some of the most egregious alleged actions (lying to anti-money laundering authorities, pretending to shut down the system while engaging in transactions, creating shell companies), the number of similarities between Liberty Reserve and Bitcoin is significant. Tellingly, after Bharara announced his action against Liberty Reserve, Patrick Murck, the General Counsel of the Bitcoin Foundation—an organization dedicated to standardizing, protecting and promoting Bitcoin—issued a statement: ''I think [the *Liberty Reserve* indictment] is just another giant, flashing warning light to Bitcoin exchanges: If you're not compliant, there are some serious risks, both at the federal and state levels.''[24] And, to help regulators understand the mechanics of Bitcoins and the Bitcoin exchanges, Murck has already held informational meetings with representatives of several U.S. government agencies.[25]

Murck's warning, while prudent, is hardly novel. Prior to the Liberty Reserve indictment, the government identified Bitcoin as a potential risk for another legal violation—money laundering. In April 2012, the FBI published a report devoted entirely to the potential for Bitcoin to be used by criminals to transfer, launder or steal funds.[26] The FBI noted that the way the Bitcoin network ''creates, operates, and distributes Bitcoins makes it distinctively susceptible to illicit money transfers, and manipulation through the use of malware and botnets.''[27] The FBI's report also highlights Bitcoin's inability to run an anti-money laundering compliance program or accept and process subpoenas and other legal requests, thereby seriously hindering the policing of suspicious monetary transactions.[28] Although not explicitly stated by the FBI, a bank that hosts Bitcoin-related accounts may face similar challenges in implementing an anti-money laundering compliance campaign.

Bringing Bitcoin to Banks—Other Potential Legal Hurdles

Bitcoin exchanges are simultaneously the weakest link in the Bitcoin chain, and the most important. Bitcoin exchanges let individuals trade Bitcoins for traditional currency; without these exchanges, integrating Bitcoin into the global economy would be practically impossible. However, because these exchanges use traditional currency and interact with regular bank accounts, they are more likely to face regulation and enforcement actions by government agencies.

While most Bitcoin exchanges are stand-alone entities, one of the greatest steps forward for Bitcoin has been the creation of a European Bitcoin bank. In late 2012, Bitcoin Central—a European Bitcoin exchange—gained approval from Banque de France, ACP (the French equivalent of the Securities and Exchange Commission) and TRACFIN (the French anit-money laundering supervising body) to become a Payment Services Provider with an International Bank ID number.[29] This approval will permit Bitcoin Central to issue debit cards and carry out electronic funds transfers, thereby allowing customers to shift funds between traditional accounts and their Bitcoin wallets.[30] Not only does this provide consumers with a one-stop portal to use their Bitcoins, but it also provides a significant degree of legitimacy to Bitcoin as a currency.

Although Bitcoin Central's recent approval abroad marks a significant step forward for Bitcoin, any U.S. bank considering the addition of Bitcoin accounts faces several hurdles. European and U.S. bank regulators are very different, and U.S. banks should be aware of several regulatory issues that may accompany the entry of either Bitcoins or a Bitcoin exchange into a bank's consumer lending portfolio. For example, the *Silk Road* complaint indicates that U.S. regulators are aware of Bitcoin's anonymity, and that institutions which appear to encourage the use of this anonymity for improper purposes may face additional scrutiny.

---

[20] Dep't of the Treasury, Notice of Finding That Liberty Reserve S.A. Is a Fin. Inst. of Primary Money Laundering Concern (May 28, 2013), *available at* http://www.fincen.gov/statutes_regs/files/311—LR-NoticeofFinding-Final.pdf.

[21] Press Release, United States Attorney's Office, S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme (May 28, 2013).

[22] *See id.*

[23] *See id.*

[24] Reed Albergotti and Jeffrey Sparshott, *U.S. Says Firm Laundered Billions*, Wall St. J. May 29, 2013, at C1.

[25] Robin Sidel, Bitcoin Group, Regulators to Meet, Wall St. J. (Aug. 25, 2013).

[26] Fed. Bureau of Investigation, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity* (2012).

[27] *Id.* at 4.

[28] *Id.* at 5.

[29] *Virtual Cash Exchange Becomes Bank*, BBC News (Dec. 7, 2012, 12:07 ET), http://www.bbc.co.uk/news/technology-20641465.

[30] *Id.*

  BBR ISSN 0891-0634

Bank Secrecy Act

The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970[31]—colloquially known as the Bank Secrecy Act—requires U.S. banks to retain borrower information and assist in money laundering investigations.

As mentioned above, Bitcoin's anonymity and privacy are in tension with a financial institution's responsibilities under the Bank Secrecy Act. The Act requires banks to keep extensive records regarding cash purchases of negotiable instruments, report suspicious activity, and file Currency Transaction Reports for all cash transactions exceeding $10,000. To comply with the Act, a bank needs a customer's first and last name, address, date of birth, social security number or taxpayer identification number, bank account number, and the amount and kind of transaction.[32] Bitcoin, however, was created to permit anonymity and privacy—for many users, this is its greatest appeal. For a bank to comply with the reporting provisions of the Bank Secrecy Act, it would have to require borrowers to forfeit this anonymity, and one important incentive for individuals to use Bitcoin would disappear.

Additionally, the Bank Secrecy Act requires money transmitting businesses to register with FinCEN.[33] Already, one Bitcoin exchange has been targeted under this provision of the Act. In May, the Department of Homeland Security seized funds held by a subsidiary of Mt. Gox—the largest Bitcoin exchange—for not being registered as a money service business with FinCEN.[34]

Furthermore, DOJ has already obtained a guilty plea against a similar service for money laundering. In 2008, E-Gold Limited and three of its directors pleaded guilty to charges of conspiracy to engage in money laundering and operate an unlicensed money transmitting business.[35] According to DOJ, E-Gold did not require users to provide their true identity and did not verify identities, even though E-Gold knew that some of its customers used the service to fund illegal activities. DOJ also claimed that E-Gold employees lacked sufficient experience to monitor accounts for criminal activity, and E-Gold encouraged customers whose criminal activity had been uncovered to transfer money to other E-Gold accounts.[36]

However, there may be an argument that the Bank Secrecy Act does not apply to Bitcoin. FinCEN regulations define ''currency'' as ''currency and coin of the U.S. or any other country as long as it is customarily accepted as money in the country of issue.''[37] Bitcoin, however, is not ''issued'' by the United States—or any other country for that matter. Instead, individuals mine their own Bitcoins through the Bitcoin algorithm; if there is any issuing authority, it would be the Bitcoin algorithm or the individual user. Furthermore, although a small number of retailers accept Bitcoins, it is unlikely that a court would hold that Bitcoin is ''customarily accepted as money.'' This argument may have a limited shelf-life, however, since the Treasury Department could easily amend the regulatory definition of ''currency''—this would undoubtedly prove less taxing than concocting an entirely new regulatory scheme for this emerging payment medium. Perhaps as a sign of changes to come, in March 2013 the Treasury Department stated that companies that issue or exchange online currency are subject to anti-money laundering rules.[38]

Miscellaneous Regulatory and Enforcement Risks

Although the risk of criminal prosecution under the Bank Secrecy Act is the greatest threat to a bank that holds Bitcoins in its deposits, Bitcoin comes with a number of other risks as well. Under Federal Reserve Board (''FRB'') rules, a bank must retain a specified ratio of deposits to loans—it is unclear if the FRB would permit Bitcoin assets to count towards this deposit amount. Similarly, although the FDIC insures deposits in foreign currency,[39] the FDIC may be wary of insuring accounts that contain Bitcoins given the lack of any sovereign support. Furthermore, it is also unclear how the Office of the Comptroller of the Currency or the Consumer Financial Protection Bureau will respond to Bitcoin accounts—at a minimum, additional regulations and disclosures appear likely. Finally, as demonstrated in the *Liberty Reserve* and *Silk Road* actions, agencies as varied as the DOJ, Internal Revenue Service, Secret Service, and the Department of Homeland Security are taking an increased interest in virtual currency exchanges and virtual currencies such as Bitcoin.

Conclusion

Bitcoin illustrates several significant challenges that virtual currencies pose for financial institutions. The answer to these challenges, however, does not lie in simply ignoring the emergence of virtual currencies. With European regulatory agencies already recognizing Bitcoin as a Payment Services Provider, the question is not if, but when and how, domestic financial institutions will attempt to integrate virtual currencies into their portfolios. Where there are risks there may also be rewards—the challenge is to manage the risks of virtual currencies in today's regulatory environment.

---

[31] 31 U.S.C. § 5311 *et seq*.

[32] Fed. Deposit Ins. Corp., DSC Risk Management Manual of Examination Policies, § 8.1-2 (2012).

[33] *See* 31 U.S.C. § 5330.

[34] Seizure Warrant, In re Seizure of the Contents of One Dwolla Account, No. 1:13-mj-01162-SKG (D. Md. Aug, 19, 2013).

[35] Press Release, Department of Justice, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges (July 21, 2008), *available at* http://www.justice.gov/opa/pr/2008/July/08-crm-635.html.

[36] Interestingly, the key defendants in the Liberty Reserve indictment are some of the same individuals involved in an E-Gold currency exchange known as Gold Age, Inc. Sealed Indictment, United States v. Liberty Reserve, S.A., No. 13 Cri. 368, ¶ 11 (S.D.N.Y. May 23, 2013).

[37] 31 CFR § 1010.100(m).

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

[39] 12 C.F.R. § 330.3(c).