LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Financial Institutions Group & White Collar Defense & Investigations Practice

December 9, 2015 | Number 1904

Enforcement Trends in Cryptocurrency

Cryptocurrency is on the rise...and so are enforcement actions.

In less than a decade, cyptocurrencies have grown from a novelty reserved for those dealing in the illicit into a robust platform embraced by financial institutions and businesses alike. Wall Street and strategic investors have increasingly taken note, working to adapt their technology, streamline market trading and integrate cryptocurrency into everyday financial transactions. The rapid adoption of cryptocurrencies has also led to increased government enforcement activity. These actions evidence US regulators' appetite to investigate fraud and other violations linked to cryptocurrency — often using traditional laws and regulations. Given this increased government scrutiny, financial institutions and traders should understand how regulators have policed the virtual world in the past in order to be prepared for the future.

Government Enforcement Actions in the Cryptocurrency Space

Unsurprisingly, government regulators, including the Securities and Exchange Commission (SEC), the Department of Justice (DOJ), the Commodities Futures Trading Commission (CFTC), the Federal Trade Commission (FTC) and the Financial Crimes Enforcement Network (FinCEN), have become increasingly active in policing the cryptocurrency space. The below enforcement actions provide a bird's-eye view of how the enforcement framework for cryptocurrencies has evolved utilizing the same statutes and regulations that have been applied to traditional securities and commodities transactions. Below is a summary of these recent enforcement actions.

1. Securities and Wire Fraud

SEC v. Trendon Shavers and Bitcoin Savings and Trust

In July 2013, the SEC charged Trendon Shavers and his company, Bitcoin Savings and Trust (BTCST), in the Eastern District of Texas with securities fraud in connection with a bitcoin-based Ponzi scheme.[1] According to the SEC, Shavers perpetrated the scheme by representing to investors that he needed bitcoins to sell to buyers who wanted to purchase large quantities of the virtual currency "off the radar." In exchange, Shavers promised large returns — generally about 1% daily or 7% weekly. In reality, however, Shavers was operating a classic Ponzi scheme, merely directing the newest investments to pay purported returns on outstanding investments and for personal use.

Notably, Shavers and BTCST argued that the bitcoin-denominated investments he offered to his investors were not "securities" and, therefore, could not be regulated by securities laws. The court disagreed, ruling that bitcoins are a legal currency (or a form of money), and thus bitcoin-based investments are subject to regulation under the Exchange Act, the Securities Act, and the rules and regulations promulgated thereunder.[2] In September 2014, the court entered final judgment against Shavers and BTCST, concluding that Shavers defrauded his investors out of more than 700,000 bitcoins, and ordered Shavers to pay more than US$40 million in disgorgement and penalties.[3] In November 2014, the US Attorney's

Office for the Southern District of New York charged Shavers criminally with securities and wire fraud.[4, 5] The criminal case against Shavers represents the first federal criminal securities fraud charges related to a bitcoin-denominated investment offering. On September 21, 2015, Shavers pled guilty to one count of securities fraud for fraudulently obtaining approximately US$800,000 in bitcoin. Shavers is expected to be sentenced on February 3, 2016.

2. Securities Violations — Failure to Register Bitcoin-Related Securities Offerings

SEC v. Erik T. Voorhees

On June 3, 2014, the SEC charged Erik T. Voorhees, a well-known bitcoin entrepreneur, with publicly offering securities in two ventures without registering the offerings. Investors paid for their shares with bitcoins. According to the SEC's administrative settlement order, the first unregistered offering occurred in May 2012 as 2,600 bitcoins were raised through the sale of 30,000 shares in FeedZeBirds (which promised to pay bitcoins to users of a social media site who forwarded its sponsored text messages). Then, in two separate offerings from August 2012 to February 2013, SatoshiDICE (which advertised itself as the largest bitcoin-betting game in the world) sold 13 million shares to the public and raised 50,600 bitcoins that were worth approximately US$722,659 at the time. The profits that Voorhees ultimately earned through the unregistered offerings totaled more than US$15,000.[6]

In his settlement with the SEC, Voorhees admitted to failing to register both the FeedZeBirds and SatoshiDICE securities offerings, in violation of Sections 5(a) and 5(c) of the Securities Act and agreed to full disgorgement of about US$15,000 in profits plus a US$35,000 civil penalty. Voorhees further consented to cease and desist from committing or causing any future violations of the registration provisions, and agreed not to participate in the issuance of any security in an unregistered transaction in exchange for any virtual currency including bitcoin for a period of five years.[7]

SEC v. BTC Trading Corporation and Ethan Burnside

On December 8, 2014, the SEC brought administrative charges against a California-based computer programmer, Ethan Burnside, in connection with his unlawful operation of two online platforms used to trade securities using virtual currencies.[8] Specifically, Burnside operated "LTC-Global Virtual Stock Exchange" and "BTC Virtual Stock Exchange" as unregistered virtual currency-denominated securities exchanges and broker-dealers that executed more than 400,000 trades.[9] Burnside also offered to sell shares of two virtual currency enterprises that he owned, without registering the offerings with the SEC. In the administrative proceeding, the SEC established that (i) Burnside operated a "virtual stock exchange" without proper registration (in violation of Section 5 of the Exchange Act), and (ii) failed to register either of his virtual exchanges as broker-dealers (in violation of Section 15(b) of the Exchange Act and Sections 5(a) and 5(c) of the Securities Act. Ultimately, Burnside settled with the SEC and agreed to pay US$58,387 in disgorgement and pre-judgment interest and a US$10,000 civil penalty in addition to accepting a two-year industry bar.

3. Dodd-Frank Act Violations — Illegal Offering of Complex Derivative Products

SEC v. Sand Hill Exchange, et al.

On June 17, 2015, the SEC announced a settlement with Sand Hill Exchange — a Silicon Valley-based online exchange that sold derivative contracts (based in valuations of private companies) and accepted payment in bitcoins — and its two founders related to their violation of certain provisions of the Dodd-Frank Act.[10] In pertinent part, the Dodd-Frank Act implemented two requirements for any security-based swaps offered to an investor who does not meet the high standard of an "eligible contract participant,"[11] namely: (i) a registration statement must be effective for the offering, and (ii) contracts must be sold on a national securities exchange.[12]

According to the SEC's administrative settlement order, Sand Hill did not limit transactions to eligible contract participants. In fact, Sand Hill actively advertised that anyone could trade on its platform. Sand Hill offered, bought and sold security-based swap contracts through its website (as opposed to a national securities exchange) in violation of the Dodd-Frank provisions that limit security-based swaps transactions with entities that do not meet the definition of an eligible contract participant. Further, the principals of Sand Hill exaggerated Sand Hill's trading, operations, controls and financial backing. In the end, Sand Hill agreed to pay a civil monetary penalty of US$20,000 to settle the charges and to cease and desist from any future violations of securities laws.[13]

4. Federal Trade Commission Enforcement

FTC v. BF Labs, Inc.

In September 2014, the FTC, filed a federal complaint in the Western District of Missouri against Butterfly Labs, a company that sold specialized computers designed to "mine"[14] bitcoins.[15] The FTC sought a permanent injunction and a temporary restraining order related to Butterfly Labs' unfair and deceptive marketing practices, in violation of Section 5(a) of the FTC Act.[16] According to the FTC complaint and subsequent court order, Butterfly Labs coaxed customers into pre-ordering specialized computers designed to mine for bitcoins, but either did not deliver the computers or delayed delivery to the point that the machines became obsolete.[17] As such, Butterfly wrongfully took in between US$20 and US$50 million from more than 20,000 consumers.

The court granted the temporary restraining order, froze Butterfly's assets and issued a permanent injunction, requiring Butterfly Labs to cease misrepresenting its products and services.[18] Butterfly was eventually allowed to resume business, but was compelled to end its pre-order business model, update its pre-order refund process, and submit regular reports to the court relating to manufacturing and customer orders.

5. Anti-Money Laundering and Bank Secrecy Act Violations

United States v. Murgio and United States v. Lebedev

On July 21, 2015, the US Attorney's Office for the Southern District of New York charged Florida-based Anthony Murgo and Yuri Lebedev with operating an unlicensed money transmitting business and conspiring to do the same. According to the complaint, Murgio and Lebedev ran the unlicensed business (Coin.mx) through both a sham front-company and a credit union, in violation of federal anti-money laundering (AML) laws and regulations.[19, 20] Specifically, Murgio and Lebedev allowed customers to exchange cash for bitcoins, knowing that their customers were transacting in the proceeds of criminal activity. Additionally, Murgio exchanged cash for bitcoins for victims of cyber-attacks in which criminals had blocked access to a victim's computer system until a bitcoin "ransom" was paid, thereby enabling the cyber-attackers to profit from their criminal activities.

In total, Coin.mx exchanged at least US$1.8 million for bitcoins for tens of thousands of customers, and failed to file the requisite suspicious activity reports (SARs)[21] for any of these transactions, in violation of federal AML laws. The cases against Murgio and Lebedev are pending.

In re Ripple Labs Inc.

On May 5, 2015, Ripple Labs Inc. and its wholly owned subsidiary, XRP II, LLC settled criminal and civil allegations of Bank Secrecy Act (BSA) violations. The US Attorney's Office for the Northern District of California and the Internal Revenue Service's Criminal Investigation Division had opened a criminal investigation, while FinCEN had brought a parallel civil enforcement action.

Ripple Labs and XRP II agreed to pay a US$700,000 total penalty ($450,000 to settle criminal issues). [22] According to the criminal settlement agreement, Ripple Labs willfully violated several requirements of the BSA by acting as a money services business (MSB) and selling its virtual currency without first registering with FinCEN, as well as by failing to implement and maintain an adequate AML program designed to prevent money launderers or terrorist financiers from using its products.[23] A Ripple Lab subsidiary also willfully violated BSA provisions by failing to implement an effective AML program and by failing to file a SAR related to several financial transactions.[24] Under the civil settlement terms, Ripple likewise admitted failing (i) to register with FinCEN as an MSB — a requirement for legally selling or exchanging virtual currency — and (ii) to satisfy other BSA requirements involving AML compliance rules and failing to file several SARs. [25]

The Silk Road Trilogy: United States v. Ulbricht

Silk Road was an online black market for everything from drugs to murder-for-hire. The core of the Silk Road prosecution centered on Ross William Ulbricht, the website's founder and designer of the bitcoin-based payment system, which facilitated the illegal commerce and concealment of identities and locations of its users. On February 24, 2013, Ulbricht was indicted in the Southern District of New York for distributing narcotics, distributing narcotics by means of the internet, conspiring to distribute narcotics, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents and conspiring to commit money laundering.[26] After a four-week jury trial, he was convicted on each of the charges, sentenced to life in prison and ordered to forfeit approximately US$184 million.[27]

United States v. Faiella and United States v. Shrem

On January 27, 2014, the US Attorney's Office for the Southern District of New York charged Robert M. Faiella (an underground bitcoin exchanger) and Charlie Shrem (the Chief Executive Officer and Compliance Officer of BitInstant, a bitcoin exchange) with selling more than US$1 million in bitcoins to users of Silk Road, thereby enabling users to make illegal purchases.[28] Faiella was charged with one count of conspiracy to commit money laundering and one count of operating an unlicensed money transmitting business. In September 2014, Faiella pled guilty and was subsequently sentenced to four years in prison, also forfeiting US$950,000. [29]

Shrem knowingly facilitated Faiella's business, allowing Faiella to buy bitcoins for Silk Road customers. Shrem failed to file SARs identifying illicit activity and helped Faiella circumvent AML restrictions. In December 2014, Shrem was sentenced to two years in prison after pleading guilty to aiding and abetting the operation of an unlicensed money-transmitting business. As part of his plea, Shrem also agreed to forfeit US$950,000 to the United States government.[30]

United States v. Force and *United States v. Bridges*

In July 2015, former DEA agent Carl Force pled guilty to charges of money laundering, obstruction of justice and extortion related to his investigation of Silk Road, after being charged in the Northern District of California in March of 2015.[31] For two years, Force worked on the Silk Road investigation, at one point serving as the lead undercover agent. Force admitted to selling Ulbricht details about the Silk Road investigation, stealing his bitcoins, extorting third parties, communicating with him via encrypted messaging and selling his story to a major motion picture studio for US$240,000. Further, Force admitted falsifying official reports and stole more than US$100,000 in bitcoins. Force also invested in CoinMKT (a cryptocurrency exchange company), covertly served as CoinMKT's Chief Compliance Officer and later misappropriated about US$300,000 from CoinMKT. In October 2015, Force was sentenced principally to 78 months' imprisonment and ordered to forfeit US$340,000, in addition to the proceeds he had already agreed to relinquish to the government.

On August 31, another former federal agent — Shaun Bridges — pled guilty to money laundering and obstruction of justice for diverting more than US$800,000 in cryptocurrency related to his investigation of Silk Road.[32] Bridges awaits sentencing. On December 7, 2015, Bridges was sentenced to 71 months' imprisonment and ordered to forfeit approximately $1.1 million.

6. CFTC Actions: Bitcoins Are Commodities

In re Coinflip

On September 17, 2015, the CFTC issued an order (Derivabit Order), filing and simultaneously settling charges against Coinflip, Inc. and its CEO with respect to Coinflip's operation of a bitcoin options trading platform (Derivabit).[33] Specifically, the Derivabit Order found that Coinflip violated the Commodity Exchange Act (CEA) by operating a facility for the trading or processing of commodity options without registering as a swap execution facility or as a designated contract market. The order marks the CFTC's first enforcement action involving bitcoin and bitcoin derivatives, and serves as a formal CFTC pronouncement that Bitcoin and other cryptocurrencies are properly classified as "commodities" under the CEA. This order provides a preview of the scope of future CFTC regulation of the cryptocurrency market.[34]

In re TeraExchange LLC

Just one week later, on September 24, 2015, the CFTC issued its second Bitcoin-related order (TeraExchange Order), filing and simultaneously settling charges against TeraExchange LLC, a swap execution facility (SEF). According to the TeraExchange Order, TeraExchange organized the execution of two prearranged and fully offsetting US$-to-Bitcoin trades with a notional amount of US$500,000 (a practice known as "wash trading") on its SEF. The trades were organized ostensibly to test TeraExchange's SEF; however, shortly thereafter, TeraExchange issued a press release announcing the first-ever bitcoin derivative transaction on a regulated exchange, without disclosing the fact that the trades were preoperational tests. According to the CFTC, the press release therefore gave the impression of actual trading and liquidity in the market.[35]

Moving Forward: What to Consider

Regulators and enforcement officials will continue to scrutinize cryptocurrency-related businesses and schemes using existing statutes and regulations. As cryptocurrency and the blockchain protocol continue to take root, companies should implement early and effective compliance and record-keeping programs to minimize the cost and impacts of compliance with possible government investigations and enforcement actions.

Cryptocurrency-related businesses should consider the following best practice points in developing any effective program.[36]

1. Regulators Have Already Enacted Robust Requirements on Cryptocurrency Businesses

That regulators have implemented recordkeeping, reporting and KYC requirements suggests that the same AML and KYC controls applicable to traditional currencies, securities and systems will apply to cryptocurrencies:

- **FinCEN.** On March 18, 2013, FinCEN confirmed that its rules pertaining to MSBs apply equally to virtual currencies.[37] Specifically, an "administrator" or "exchanger" of virtual currency must register as an MSB and is subject to BSA recordkeeping obligations. Virtual currency MSBs must assess their risk of money laundering or terrorist financing as part of a general anti-money laundering plan.[38] They must also keep records on both the transmitter and the receiver for any money transfer of US$3,000 or more. Further, MSBs must keep a record, including a customer's name and address, for each exchange of currency for transactions greater than US$1,000.[39]

- **New York's BitLicense.** The BitLicense requires a comprehensive AML program.[40] This program includes:

  - **Risk Assessment:** Initial and yearly (or more frequently "as risks change") assessments considering legal, compliance, financial and reputational risks

  - **Dedicated Compliance Function:** System of internal controls, policies and procedures to ensure compliance with AML laws, rules and regulations, including a dedicated AML compliance officer

  - **Audit Function:** Regular independent audit for compliance with and effective of AML program

  - **Prohibitions:** Disallows assisting, aiding or allowing transactions aimed at avoiding reporting requirements

  - **Records:** Requires retention, for at least seven years, of detailed records including the identity and physical address of the licensee's customers/account holders and other parties to the transaction; the amount of the transaction; and other details related to transaction, including date, description and method of payment

  - **Reporting Requirement:** Requires notification to NYDFS within 24 hours if virtual currency transactions exceed US$10,000 in a single day; SARs must be filed within 30 days if licensee is not subject to federal SAR requirement

  - **Office of Foreign Assets Control (OFAC) Compliance:** Requires cross-checking all customers against OFAC's Specially Designated Nationals (SDN) list

  - **Customer Identification Program:** Must reasonably identify/verify a customer's identity, including name and physical address

- Several states (including Connecticut) require that a cryptocurrency business obtain a money transmitter license.

- Increasingly, other states, including California, are implementing cryptocurrency laws and regulations modeled on the BitLicense.[41]

2. Recordkeeping Requirements

Strict recordkeeping requirements are both a challenge and an imperative for any business using cryptocurrency. While transactions in cryptocurrencies (like bitcoin) are private and encrypted, they are not totally anonymous. As the use and adoption of cryptocurrency grows and continues to undergo legal and regulatory scrutiny — particularly with regard to compliance with AML statutes and know-your-customer (KYC) controls — transactions will yield increased data attributable to the parties to a transaction. That transaction data should be properly stored and organized to ensure compliance with these recordkeeping requirements.

3. Know-Your-Customer Requirements

Cryptocurrency businesses deemed money transmitters are subject to certain KYC requirements.[42] KYC policies require financial institutions to verify the identity of their customers, determine and verify the identity of any beneficial owner and understand the origin of transmitted funds. Besides the costs associated with completing this diligence, KYC rules likely will materially impact virtual currency as anonymity is a key selling point for many customers, and as transactions occur on a global scale with near-immediate settlement terms. Thus, businesses must develop a robust KYC policy that balances consumer privacy on the one hand and regulatory requirements requiring a baseline knowledge of all parties to a transaction on the other.

4. Reporting Requirements

Financial institutions and money service businesses (MSBs) are required to monitor transactions and file reports if a transaction meets certain thresholds or in cases of certain suspicious activity. The same requirements apply to those involved in cryptocurrency transactions. All MSBs must file Currency Transaction Reports (CTR) on customer cash transactions exceeding US$10,000 in a single day. These CTRs must include information about the account owner's identity and occupation. MSBs must also file a Currency or Monetary Instruments Report (CMIR) for transporting, mailing or shipping a monetary instrument in an amount in excess of US$10,000. Separate and apart from CTRs, financial institutions and MSBs must file a SAR for activity that is for US$2,000 or more and is "suspicious." Financial institutions and cryptocurrency-related businesses must ensure that their reporting infrastructure applies with equal force to transactions involving cryptocurrency.

5. Anti-Money Laundering Laws

Of course, compliance with the various anti-money laundering laws and regulations is also essential. These laws apply to any person or business, regardless of whether they are a financial institution or a MSB. Thus, businesses must also be mindful of these rules and regulations to ensure proper compliance.

Conclusion

Recent enforcement actions demonstrate that existing laws and regulations apply with equal force to businesses and financial institutions transacting in cryptocurrency. Businesses built upon or using cryptocurrencies should be mindful to implement strict internal controls and compliance standards and comply with relevant regulatory requirements in order to build successful businesses outside of a regulators' crosshairs. No doubt, in the coming years, cyptocurrencies will face increasing scrutiny, and thus it behooves both businesses and legal practitioners to monitor the enforcement and regulatory landscape.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Benjamin Naftalis
benjamin.naftalis@lw.com
+1.212.906.1713
New York

Alan W. Avery
alan.avery@lw.com
+1.212.906.1301
New York

Vivian A. Maese
vivian.maese@lw.com
+1.212.906.1302
New York

Stephen P. Wink
stephen.wink@lw.com
+1.212.906.1229
New York

Yvette Valdez
yvette.valdez@lw.com
+1.212.906.1797
New York

Yulia M. Fradkin
yulia.fradkin@lw.com
+1.212.906.1279
New York

Matthew S. Salerno
matthew.salerno@lw.com
+1.212.906.4738
New York

You Might Also Be Interested In

Regulating Bitcoin and Other Cryptocurrencies

Cryptocurrencies Are Commodities: CFTC's First Bitcoin Enforcement Action

Regulatory Notes on Bitcoin and Other Cryptocurrency Derivatives

Virtual Currencies: New York State Department of Financial Services Discusses Proposed Regulations

GMAC/CFTC Hosts Open Meeting Regarding Bitcoin and Digital Currency

Endnotes

[1] *SEC v. Shavers and Bitcoin Savings and Trust*, 13-CV-416 (E.D. Tex. filed July 23, 2013), https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf. The SEC Complaint alleged violations of Section 17(a) of the Securities Act, Section 10(b) of the Exchange Act and Rule 10b-5 thereunder, and Section 5(a) and 5(c) of the Securities Act. *See also, SEC v. Shavers*, No. 4:13-CV-416, Litigation Release No. 23090 (E.D. Tex. Sept. 22, 2014), available at http://www.sec.gov/ligigation/litreleases/2014/lr23090.htm.

[2] *SEC v. Shavers*, No. 4:13-CV-416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013) ("Bitcoin is a currency or form of money, and investors wishing to invest in BTCTS provided an investment of money.").

[3] https://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

[4] *United States v. Shavers*, 14 Mag. 2465 (S.D.N.Y. filed Nov. 3, 2014), http://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Shavers%2C%20Trendon%20Complaint.PDF.

[5] Benjamin Naftalis, an author of this article, investigated and charged this case while serving as an Assistant United States Attorney in the Southern District of New York.

[6] Press Release, SEC, SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities (June 3, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520.

[7] *Id.*

[8] Press Release, SEC, SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations (Dec. 8, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543655716.

[9] BTC Trading, Corp. and Ethan Burnside, Securities Act Release No. 9685 (Dec. 8, 2014), http://www.sec.gov/litigation/admin/2014/33-9685.pdf.

[10] Securities Act Release No. 9685 (Dec. 8, 2014); Press Release, SEC, SEC Announces Enforcement Action for Illegal Offering of Security-Based Swaps (June 17, 2015) http://www.sec.gov/news/pressrelease/2015-123.html.

[11] 7 U.S.C. § 1a(18) (2010).

[12] 15 U.S.C. § 77e (2012).

[13] Sand Hill Exchange, Gerrit Hall, and Elaine Ou, Securities Act Release No. 9808 (June 16, 2015), https://www.sec.gov/rules/other/2015/33-9808.pdf.

[14] "Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the block chain, and also the means through which new bitcoin are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin." Investopedia.com, Bitcoin Mining, http://www.investopedia.com/terms/b/bitcoin-mining.asp (last visited Nov. 9, 2015).

[15] Complaint, FTC v. BF Labs, Inc., *et al.*, No. 4:14-cv-00815-BCW (W.D. Mo. Sept. 15, 2014), https://www.ftc.gov/system/files/documents/cases/140923utterflylabscmpt.pdf.

[16] 15 U.S.C. § 45(a).

[17] Press Release, FTC, At FTC's Request, Court Halts Bogus Bitcoin Mining Operation (Sept. 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/ftcs-request-court-halts-bogus-Bitcoin-mining-operation.

[18] Ex Parte Order, FTC v. BF Labs, Inc., *et al.*, No. 14-cv-00815-BCW (W.D. Mo. Sept. 18, 2014), https://www.ftc.gov/system/files/documents/cases/140923utterflylabstro.pdf.

[19] Press Release, FBI, Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange (July 21, 2015), https://www.fbi.gov/newyork/press-releases/2015/manhattan-u.s.-attorney-announces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange.

[20] Complaint, United States v. Murgio, No. 1:15-MJ-02508 (S.D.N.Y. July 17, 2015), http://www.justice.gov/usao-sdny/file/632166/download; Complaint, *United States v. Lebedev*, 1:15-MJ-02501 (S.D.N.Y. July 17, 2015), http://www.justice.gov/usao-sdny/file/632161/download.

[21] A suspicious transaction: (1) involves funds derived from illegal activity; (2) is designed to evade any requirements of the BSA; or (3) serves no business or other lawful purpose. 31 C.F.R. § 1022.320.

[22] Press Release, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), http://www.fincen.gov/news_room/nr/html/20150505.html.

[23] Settlement Agreement, In re Ripple Labs Inc., No. 2015-05 (May 5, 2015), http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf.

[24] *Id*.

[25] Assessment of Civil Money Penalty, In re Ripple Labs Inc., No. 2015-05 (May 5, 215), http://www.fincen.gov/news_room/nr/pdf/Ripple_Assessment.pdf.

[26] Indictment, *United States v. Ulbricht*, No. 14-CR-068 (S.D.N.Y. Feb 4, 2014), http://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.

[27] Press Release, DOJ, Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), http://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

[28] Press Release, DOJ, Manhattan U.S. Attorney Announces Charges against Bitcoin Exchangers, Including CEO of Bitcoin Exchange Company, for Scheme to Sell and Launder over $1 Million in Bitcoins Related to Silk Road Drug Trafficking (Jan. 27, 2015), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-Bitcoin-exchangers-including-ceo.

[29] Press Release, DOJ, Bitcoin Exchanger Sentenced in Manhattan Federal Court to Four Years in Prison for Selling Nearly $1 Million in Bitcoins for Drug Buys on Silk Road (Jan. 20, 2015), http://www.justice.gov/usao-sdny/pr/Bitcoin-exchanger-sentenced-manhattan-federal-court-four-years-prison-selling-nearly-1.

[30] *Id*.

[31] Press Release, FBI, Former Silk Road Task Force Agent Pleads Guilty to Extortion, Money Laundering, and Obstruction, (July 1, 2015), https://www.fbi.gov/sanfrancisco/press-releases/2015/former-silk-road-task-force-agent-pleads-guilty-to-extortion-money-laundering-and-obstruction.

[32] *Id*.

[33] *In re Coinflip, Inc., d/b/a/ Derivabit, et al.*, CFTC No. 15-29, Comm. Fut. L. Rep. P 33538, 2015 WL 5535736 (Sept. 17, 2015), http://www.cftc.gov/ucm/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf (hereinafter Derivabit Order).

[34] *Id.*

[35] *In the Matter of TeraExchange LLC*, CFTC No. 15-33 Comm. Fut. L. Rep. P 33546, 2015 WL 5658082 (Sept. 24, 2015), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfteraexchangeorder92415.pdf (hereinafter TeraExchange Order).

[36] Of course, these best practice suggestions are in addition to, and not in lieu of, the compliance, KYC, reporting and recordkeeping requirements which the SEC and the CFTC, among others have mandated.

[37] Guidance, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013).

[38] 31 C.F.R. § 1022.210 (2006).

[39] 31 C.F.R. §§ 1010.311-1010.312 (2015).

[40] BitLicense §§ 200.12(a), 200.15 (2015).

[41] Assem. Bill 1326, 2015-2016 Reg. Sess. (cal. 2015) (amended in Senate Aug. 18, 2015) (hereinafter California BitLicense).

[42] 31 U.S.C. § 5318(i) (2006).