THOMSON REUTERS

Westlaw®

Fintech in Focus: Anti-Money Laundering Regulatory Developments for Virtual Currencies and Initial Coin Offerings

Obiamaka P. Madubuko and Margaret Ukwu, *Greenberg Traurig**

MARCH 15, 2018

Virtual currencies like Bitcoin and Ether are new entrants into the global financial services industry while initial coin offerings (hereinafter "ICOs") are opening up new ways for businesses to access capital using blockchain technology. These new technologies pose real concerns regarding anti-money laundering (hereinafter "AML"), fraud and security risks. This article will explore AML regulatory developments and enforcement trends for virtual currencies and ICOs in the United States and offers insights for what fintech companies can do to minimize their AML, fraud and security risks.

VIRTUAL CURRENCIES AND BLOCKCHAIN TECHNOLOGY

Virtual or cryptocurrencies are digital assets created and managed using blockchain technology. These online currencies are not recognized by any jurisdiction, yet they can have real value for investors who have the appetite for their high volatility. For example, Bitcoin, the world's first and most popular cryptocurrency created in 2009, has had huge swings in value in recent months. According to a February 3, 2018 CNBC report, the cryptocurrency market recently suffered a massive $100 billion loss in value sending Bitcoin prices to below $8,000 per coin, after reaching a record high of $19,000 in December 2017. See Arjun Kharpal, Cryptocurrency market stabilizes after violent sell-off, CNBC (Feb. 3, 2018, 6:32 AM), http://www.cnbc.com/2018/02/03/bitcoin-price-cryptocurrency-market-stabilizes-after-violent-sell-off.html (last visited Mar. 15, 2018).

Blockchain technology is a digital ledger system used to verify, process and store records/transactions (called blocks) that are linked by a group of connected computers (called nodes) and secured using cryptography. A core feature of blockchain is that it has no central authority and is decentralized, allowing users to identify themselves only by their public key. All participants to a transaction have access to the blockchain, which is intended to serve as an immutable record of the transaction. Blockchains may be public (open-sourced) or private (accessible only to certain authorized users). Given that blockchain users do not need to know one another in order to engage in transactions, some have called blockchain networks "trustless" systems whereas blockchain enthusiasts argue that such networks provide "more trust" because these transactions are fully transparent and accessible by all transaction participants in real time.

Virtual currencies are not only a form of blockchain technology, they are also a method of payment for parties to use a blockchain network. Investors have begun to buy and hold these cryptocurrencies betting that their value will increase as blockchain technology gains greater acceptance and adoption by consumers and businesses.

INITIAL COIN OFFERINGS (ICOS)

ICOs are the latest blockchain phenomenon to disrupt the financial services industry. An ICO is an online capital-raising campaign that offers and sells cryptocurrency (called tokens or coins), which are used to finance new projects or to provide access to a company's platform or services. ICOs offer greater access to capital and enable business start-ups and online projects to raise funds in a short time period without having to sell stock or give away equity. For example, in August 2017, Filecoin, a blockchain-based storage network startup, raised almost $188 million in just 60 minutes. According to a December 18, 2017 New York Times article, ICOs raised over $4 billion in 2017, a 3,000% increase over ICO funds raised in 2016. See John Patrick Mullin, ICOs In 2017: From Two Geeks And A Whitepaper To Professional Fundraising Machines, Forbes.com (Dec. 18, 2017, 11:29 PM), http://www.forbes.com/sites/outofasia/2017/12/18/icos-in-2017-from-two-geeks-and-a-whitepaper-to-professional-fundraising-machines/#17ab8978139e (last visited Mar. 15, 2018).

AML RISKS FOR VIRTUAL CURRENCIES AND ICOS

A chief concern for virtual currencies and ICOs is AML risk. Given that ICOs involve the online offer and sale of tokens (i.e., virtual

currencies) conducted with limited (if any) central oversight, these potentially global investment platforms represent unique challenges for U.S. regulators.

The AML and fraud risks associated with virtual currencies and ICOs are multi-fold.

First, fraud and token theft remain looming concerns for any ICO offering or virtual currency owner. For example, Veritaseum, the issuer of a cryptocurrency called VERI, fell victim to a July 2017 hack in which $8 million worth of VERI were stolen. Coindash, an Israeli startup, planned to raise capital by selling its tokens in exchange for ether (another digital currency). However, just 13 minutes into the ICO, hackers stole $7 million worth of ether by hacking Coindash's website and changing the address for investments to a fake one.

Second, customer identification and transaction verification present unique challenges, particularly given that token holders can be pseudonymous (identified by something other than their real name) making AML compliance difficult. The speed of such transactions, including the advent of smart contracts (computer code driven set of rules for self-executing and self-enforcing contracts), creates added challenges for regulators. Without the ability to accurately identify and track users and authenticate and authorize blockchain transactions, there is a heightened risk that virtual currencies and ICOs could be used to finance criminal activities or sponsor terrorism. Think of Bitcoin's sorted past with Silk Road, a notorious online drug marketplace, before it was shut down in 2013. In addition to the national and global security interests in ensuring virtual currencies and ICOs are AML compliant, these transactions also pose additional legal issues relating to taxation, cybersecurity, data privacy and data transfer.

Third, the international scope of virtual currencies and ICOs, particularly those organized offshore, represents a further regulatory challenge. The difficulty in tracing, freezing or securing cryptocurrency assets makes it hard for regulators to take action to hold those who violate the law accountable. Add to this the lack of a central authority in blockchain transactions, a lack of investor protection, and extreme volatility in cryptocurrency value, and the AML challenges multiply. It is no surprise that many regulators around the world have issued cautionary guidance for ICO investments and certain jurisdictions like China have banned them outright.

CURRENT REGULATORY LANDSCAPE

A. Federal Regulations

Currently, there is no comprehensive U.S. federal regulation specifically governing virtual currencies and ICOs. However, several federal agencies have provided guidance and some have brought enforcement actions based on existing regulations. For example, the Internal Revenue Service (IRS) has stated that virtual currencies should be treated as property and the Commodity Futures Trading Commission (CFTC) has found that some virtual currencies fall within the definition of a commodity and, thus, are subject to CFTC enforcement actions. In January 2017, the Financial Industry Regulatory Authority (FINRA) issued a report on the potential implications of blockchain technology for the securities industry. In July 2017, the SEC issued an investigation report in the DAO case determining that the DAO tokens offered in an ICO qualified as securities and laying out a roadmap for future offerings to follow consistent with existing securities laws. See U.S. Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (Release No. 81207) (July 25, 2017) https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Mar. 15, 2018). In recent months, the SEC has taken enforcement action against several ICO related companies, and SEC Chairman Jay Clayton publicly commented that, "I have yet to see an ICO that doesn't have a sufficient number of hallmarks of a security," thus making it clear that enforcement of non-compliant ICO related activity will be a key SEC enforcement priority for 2018.

The Financial Crimes Enforcement Network (FinCEN) is the chief U.S. regulator for AML law enforcement. The Bank Secrecy Act (BSA) is the primary U.S. anti-money laundering law, which requires all money service businesses (MSBs) to register with the U.S. Treasury Department, implement AML compliance programs and adhere to certain record-keeping and reporting requirements such as the filing of suspicious activity reports (SARs) and currency transaction reports (CTRs) for transactions over certain dollar amounts. Banks and other financial institutions are also required to have customer identification programs in place and to undertake customer due diligence commonly known as KYC (Know Your Customer) obligations, as mandated by the U.S. PATRIOT Act.

In 2013, FinCEN issued guidance on virtual currencies finding that virtual currency administrators and exchangers (as opposed to simply users/owners of cryptocurrencies) are considered MSBs and thus subject to BSA registration and reporting requirements. FinCEN regulations also extend to all ICOs and any transaction where a virtual currency is being exchanged for another cryptocurrency or fiat currency.

In 2015, FinCEN brought its first civil enforcement action against a virtual currency exchanger, Ripple Labs Inc. Despite no allegation of any actual fraud or theft, Ripple Labs was fined $700 million for selling its virtual currency, known as XRP, without registering with FinCEN and without

implementing an effective AML program. Ripple Labs also forfeited $450 million to resolve possible criminal violations.

B. State Regulations

In addition to these federal regulations, virtual currencies and ICOs must also comply with applicable state securities and MSB laws. Currently, each state regulates MSBs under their own laws. Some states like New York require companies that offer or sell virtual currencies to New York residents or wish to conduct an ICO to apply for a special BitLicense.

Other states (like California) are following New York's lead and have proposed legislation along the same lines. Florida recently passed House Bill 1379 clarifying the definition of virtual currency and Alabama and Washington recently updated their laws to include digital currency in the definition of money transmission. Illinois has issued digital currency guidance and Hawaii has shut down a virtual currency exchange, Coinbase, for failing to adhere to state law on cash reserves needed.

In 2015, the Conference of State Bank Supervisors (CSBS) drafted a model regulatory framework to address certain virtual currency activities, which includes among other things, a requirement that states require verification of an entity's service user, not only account holders as part of the customer identification process.

FUTURE REGULATORY TRENDS

So what to expect in the future? It is safe to say, as more regulators continue to weigh in on the cryptocurrency space, more regulation is expected. In 2016, a bi-partisan group of U.S. Congress members established a blockchain caucus understanding the potential for blockchain and the need for new laws to support this new technology. The federal Office of the Comptroller of the Currency (OCC) has proposed a special purpose bank charter for crypto-exchanges and other fintech companies. This special purpose charter would pre-empt state-by-state licensing laws for fintech businesses but would not be subject to FDIC protections. Certain state regulators, including the California Department of Business Oversight and NYS DFS have resisted the OCC's fintech charter, claiming that it represents an impermissible overreach by the federal government that will serve to weaken state enforcement of consumer protection laws. On December 12, 2017, a New York federal court dismissed the NYS DFS claims, finding the court lacked jurisdiction as the OCC had not yet taken any final action.

At the state level, the Uniform Law Commission has proposed a Virtual Currency Businesses Act (VCBA) to promote uniform state laws for cryptocurrency related businesses. The VCBA drafting committee will consider licensing requirements, reciprocity, consumer protection, cybersecurity, AML/KYC, and supervision of licensees.

CONCLUSION

In this new era of ICOs, cryptocurrencies and blockchain transactions, managing AML, fraud and security risks will remain top-of-mind for fintech companies seeking to gain investor confidence and will remain an active area for government regulators for the foreseeable future.

Fintech companies would be wise to incorporate "security by design" features into their proposed projects, to consider security from inception through launch, and to voluntarily adopt AML/KYC processes that meet U.S. federal regulations while continuing to improve processes for verifying and storing user/customer identification and data. Government regulators and legislators, in turn, should enact smart regulations that are not overly burdensome or hamper innovation but are designed to keep consumers safe and create accountability for wrongdoers. This space will likely continue to generate a lot of interest and activity by regulators, consumers and fintech companies in the years to come.

This article first appeared in Westlaw's publication entitled Payment Systems and Electronic Fund Transfers Guide. The publication is part of the Emerging Areas of Practice Series – a new publishing initiative which reduces product to market time to cover emerging areas of the law as they develop. New documents are loaded to Westlaw on a rolling basis as received and content is updated quarterly.

ABOUT THE AUTHORS

Obiamaka P. Madubuko is a shareholder in **Greenberg Traurig**'s New York office. She focuses her practice on anti-corruption and fraud matters and advises U.S.-based companies doing business in international markets. She advises companies on a host of compliance and transactional due diligence issues arising under the Foreign Corrupt Practices Act (FCPA), UK Bribery Act, the Dodd-Frank Act, Office of Foreign Asset Control (OFAC) and other global trade regulations, including cybersecurity defense and data breach response. She also assists clients with internal investigations, risk assessments and independent audits, as well as drafting, evaluating and updating corporate policies to ensure compliance.

In addition to her significant corporate advisory practice, Obi is an experienced trial lawyer who has defended individuals and corporations in complex civil litigation and white collar criminal cases. She has represented clients before state and federal courts and agencies, including the United States Congress, the United States Department of Justice, the U.S. Securities and Exchange Commission, the Equal Employment Opportunity Commission, the Federal Election Commission, and other federal and state authorities.

Margaret Ukwu is a law clerk/JD in **Greenberg Traurig's** New York office. She focuses her practice on complex patent litigation and prosecution involving medical devices, pharmaceuticals, consumer products, electronics and a broad range of technologies pertaining to mechanical systems and devices, complex integrated circuits, semiconductors, signals processing, computer architecture, software and user interfaces. She has also assisted in writing and implementing new law in Uganda and Rwanda.

In addition to her legal work, Margaret is an experienced control systems engineer. She has worked on projects involving liquefied natural gas plants, vitrification plants and chemical agent destruction and demilitarization plants.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.