THOMSON REUTERS

Westlaw®

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

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

MAY 30, 2019

Virtual currencies like Bitcoin and Ether are new entrants into the global financial services industry. ICOs (initial coin offerings) are opening 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.

While no U.S. federal law specifically addressing ICOs or virtual currencies was passed in 2018, enforcement efforts by federal and state regulators against ICOs and cryptocurrency administrators and exchangers are on the rise, indicating that a "regulation-through-litigation" trend is likely to continue in 2019.

VIRTUAL CURRENCIES AND BLOCKCHAIN TECHNOLOGY

Virtual or cryptocurrencies are digital assets created and managed using blockchain technology. These online currencies 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 was created in 2009, and has had huge swings in value in the past year. At the end of Dec. 2018, Bitcoin (BTC) was trading around $4100 per coin, a nearly 80% drop in value after reaching a record high of $19,000 per coin in Dec. 2017. See https://www.tradingview.com/symbols/BTCUSD/ (last visited Dec. 21, 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 form of encryption). A core feature of blockchain is that it is decentralized. 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/permissioned (accessible only to certain authorized users). Given that blockchain users do not need to know one another to engage in transactions and may be identified on the blockchain only by their public key, 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 (or access) that enable 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, now more commonly referred to as STOs (security token offerings), are the latest blockchain phenomenon to disrupt the financial services industry. An ICO or STO, generically called a token offering, is typically structured as 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. Coin offerings often take the form of a "pre-sale" offering, using a derivative or other instrument that converts into the tokens at the initial generation event. Pre-sales facilitate access to capital and enable business start-ups and online projects to raise funds in a short time period, generally without having to give away equity in the underlying entity. Most pre-sales and ICOs are limited to accredited investors to qualify for exemptions from federal and state securities laws in the United States.

May 2019 Update: There is a growing trend towards ICOs voluntarily complying with SEC and state securities laws prior to a launch to avoid potential compliance or regulatory hurdles. These offerings, called STOs, are ICOs that comply with U.S. securities laws. The STO trend is expected to continue in 2019.

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. Criminals prefer to use virtual currencies because they are not tied to a single jurisdiction or set of laws, exchanges can be handled quickly and pseudonymously, and there is no need to rely on intermediaries and, in many cases, there is no central authority to monitor these exchanges.

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 act to hold those who violate the law accountable. Add to this the lack of a central authority in many 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.

AML REGULATORY LANDSCAPE FOR VIRTUAL CURRENCIES AND ICOS

While federal and state agencies are developing new approaches to AML compliance, there is no standard set of rules that govern this emerging technology. Under the current US regulatory landscape, there are different, sometimes inconsistent, approaches among federal and state agencies regarding enforcement of virtual currencies and ICOs.

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 Jan. 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 Securities and Exchange Commission (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 2018, the SEC initiated several enforcement actions against various ICO related companies, yet it has not, to date, issued any specific regulations governing ICOs or virtual currencies opting instead to enforce existing securities law regulations against virtual currency companies and ICOs as it deems appropriate. Given this ambiguity, the regulatory landscape remains unclear.

The Financial Crimes Enforcement Network (FinCEN), which is under the U.S. Treasury Department, 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.

May 2019 Update: On May 9, 2019, FinCEN issued a new guidance on virtual currencies entitled Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVCs) (hereafter, "2019 FinCEN Guidance"). See FinCEN Press Release (May 9,

2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf (last visited May 27, 2019). This guidance updates FinCEN's 2013 guidance on virtual currencies and represents a consolidated set of the rules and regulations issued by FinCEN since 2011. Notably, the 2019 FinCEN Guidance explores various business models and explains FinCEN's regulatory approach as to which models may qualify as money transmitters and which ones may be exempt. For example, the following business models may qualify as money transmitters: (1) P2P Exchangers (except if making infrequent transactions not for gain), (2) Hosted Wallet Providers, (3) CVC Kiosks that exchange CVC for real currency or other CVC, (4) Distributed Apps that transmit money either for profit or not-for-profit, (5) Anonymity Enhanced CVC Service Providers (if transacting CVC exchanges) and (6) Payment Processing Services using CVC.

The 2019 FinCEN Guidance also discussed some specific business models involving CVC transactions that may be exempt from being defined as money transmitters under FinCEN's rules. For example, a preferential ICO sale to a select group of preferred buyers may qualify for such an exemption, however, such determinations are highly fact-dependent and the circumstances must meet an express exemption under FinCEN's definitions. See FinCEN Press Release at 24.

Lastly, the 2019 FinCEN Guidance confirmed that 31 CFR 1010.410(e) and (f), more commonly referred to as the Funds Transfer Rule and the Funds Travel Rule respectively, will also apply to transfers of CVC by money transmitters in the United States. This means that anyone issuing digital tokens will need to address money transmitter requirements, including the applicability of additional recordkeeping and reporting requirements for financial institutions and their intermediaries. For financial institutions that engage in pseudonymous virtual currency transactions (where the full name of the transmitter is replaced with a numeric code), the 2019 FinCEN Guidance affirmatively states that such transactions do not comply with obligations under the Funds Travel Rule, which represents a significant compliance hurdle for mixers and tumblers (persons/companies that engage in anonymity-enhanced virtual currency transactions), and financial institutions accepting such transactions.

In addition to the 2019 FinCEN Guidance, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced in March 2018 that it may add virtual currency identifiers associated with blocked persons to its Specially Designated Nationals (SDN) listing. In its March 2018 guidance, OFAC stated that any foreign virtual currency transaction must comply with OFAC (Office of Foreign Assets Control) sanctions rules. See OFAC FAQs: Questions on Virtual Currency, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs (last visited on Dec. 17, 2018), at 560 & 562. On Nov. 28, 2018, OFAC added certain virtual currency addresses associated with blocked persons to its SDN listing. See Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/news/press-releases/sm556; OFAC Sanctions List Search, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=7372 (as of Mar. 31, 2019).

B. State Regulations

In addition to U.S. federal regulations, virtual currencies and ICOs must also comply with applicable U.S. state securities and MSB laws.1 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, which include certain AML compliance obligations. To date, the New York State Department of Financial Services has issued 14 BitLicenses. See NYS DFS Press Release, DFS Grants Virtual Currency and Money Transmitter License to NYDIG Execution, LLC, available at https://www.dfs.ny.gov/about/press/pr1811141.htm (last visited on Dec. 17, 2018).

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, 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.

In contrast to the dearth of federal legislation specifically for ICOs and cryptocurrency, state lawmakers have been active in proposing new laws to address cryptocurrencies and ICOs in their respective jurisdictions, including whether such ventures are considered money transmitters under state law. Below are a few examples of recently enacted or proposed virtual currency and ICO related state laws that either expressly qualify (or exempt) such activities as money transmitters under state law.

ALASKA

On March 14, 2017, Alaska House Bill 180 was introduced. The Act set out to define virtual currencies. If enacted, it could potentially make cryptocurrency firms be considered a money transmitter or currency exchange requiring a license. It has

been referred to the Judiciary. See https://legiscan.com/AK/bill/HB180/2017 (last visited May 31, 2019).

COLORADO

On May 8, 2018, Colorado state senate voted and approved HB 1426, which offered guidelines to distinguish between tokens and securities and would have exempted virtual currency from state money transmitter laws, but then state lawmakers took another vote on May 9, 2018, and rejected it. See http://leg.colorado.gov/bills/hb18-1426 (last visited May 31, 2019). On Jan. 4, 2019, the Colorado legislature introduced bill SB19-023 entitled the Colorado Digital Token Act, then passed the bill on March 6, 2019. See http://leg.colorado.gov/bills/sb19-023 (last visited May 31, 2019). The bill seeks to exempt virtual currencies from the state's securities laws. This action is at odds with recent efforts by the Colorado Division of Securities, whose ICO Task Force has brought enforcement actions against 20 ICOs it claims are operating illegally in the state. See https://www.colorado.gov/pacific/dora/colorado-ico-cases-filed (last visited May 31, 2019).

ILLINOIS

The Illinois Department of Financial and Professional Regulation issued guidance regarding digital currencies on June 13, 2017. They stated that "a person or entity engaged in the transmission of solely digital currencies, as defined, would not be required to obtain a TOMA [Transmitters of Money Act] license." See https://www.idfpr.com/Forms/DFI/CCD/IDFPR%20-%20Digital%20Currency%20Regulatory%20Guidance.pdf (last visited May 31, 2019).

RECENT VIRTUAL CURRENCY ENFORCEMENT TRENDS

A. Federal Enforcement Trends

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. In 2017, BTC-e, a foreign based Bitcoin exchange, was criminally and civilly prosecuted for money laundering and assessed a $110 million by FinCEN. BTC-e executives are currently facing criminal charges relating to their actions regarding the exchange. See Steve Hudak, FinCEN Press Release (July 27, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware (last visited Dec. 21, 2018).

SEC enforcement co-directors Stephanie Avakian and Steven Peikin have stated that fraudulent ICOs are among the greatest risks currently facing investors. See Stephanie Avakian and Steven Peikin, Oversight of the SEC's Division of Enforcement, (May 16, 2018), https://www.sec.gov/news/testimony/testimony-oversight-secs-division-enforcement (last visited June 8, 2018). In Sept. 2017, the SEC created a special cyber unit within its Division of Enforcement. The SEC's cyber unit's first enforcement action came in Dec. 2017 when it obtained an emergency asset freeze to shut down a $15 million fraudulent ICO. In Jan. 2018, the SEC's cyber unit again successfully obtained an emergency asset freeze against AriseBank, a Texas-based ICO that claimed to have raised $600 million. In April 2018, it froze $27 million in trading proceeds of Longfin, a Nasdaq-listed blockchain company, in a case alleging Longfin trades violated existing securities laws.

Whether digital tokens and coins are securities or commodities subject to regulation by the SEC and CFTC remains an unresolved issue and continues to be litigated through the courts. A New York federal district court recently dismissed SEC fraud charges against a businessman for alleged misstatements he made to attract ICO investors. The court found the digital tokens at issue were not securities. See Dunstan Prial, Ruling on What Isn't a Security Needed For ICO Clarity, (May 9, 2018, 7:31 PM), https://www.law360.com/articles/1042159?scroll=1 (last visited May 19, 2018).

The CFTC has also been active in its enforcement efforts. In March 2018, the United States District Court in the Eastern District of New York held that virtual currencies can be regulated by CFTC as a commodity. The court noted, however, that the CFTC's jurisdictional authority did not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities. See No. 1:18-cv-00361-JBW-RLM, Dkt. No. 29 (E.D.N.Y. Mar. 6, 2018). In May 2018, the CFTC and the U.S. Department of Justice launched a criminal investigation into potential cryptocurrency market manipulation.

In addition to policing U.S.-based ICOs and cryptocurrency related activity, the U.S. has also taken recent action regarding foreign cryptocurrencies. For example, on March 19, 2018, President Trump issued an Executive Order prohibiting transactions with any digital currency, coin or token issued by, for or on behalf of the Venezuelan government, including the petro. See Stinebower, New Executive Order Adds New Sanctions Against Venezuela's Petro Cryptocurrency, (March 27, 2018), https://www.cmtradelaw.com/2018/03/new-executive-order-adds-new-sanctions-against-venezuelas-petro-cryptocurrency/ (last visited May 21, 2018).

The IRS has also entered the enforcement arena. New tax implications are arising for token users and purchasers. After Jan. 1, 2018, exchanging or trading one virtual currency for another became a taxable event. In March 2018, the IRS issued a bulletin mentioning that the failure to report the income tax of virtual currency transactions could result in penalties or, in more extreme situations, a prison term and a fine. In 2017, the IRS brought an enforcement action

against a virtual currency exchange that led to a federal court ordering the turnover of certain customer information to the government, signaling that the IRS may be looking to identify potential tax evaders through their virtual currency profits.

In Sept. 2018, FINRA filed its first disciplinary action involving the alleged unlawful distribution of an unregistered virtual currency security. They claimed that the company's owner, Timothy Tilton Ayre, bought the rights to a cryptocurrency, HempCoin, repackaged it as a security backed by his company's stock, then defrauded investors by making materially false statements and omissions regarding his business, HempCoin, and the state of the company's financials. See FINRA Charges Broker with Fraud and Unlawful Distribution of Unregistered Cryptocurrency Securities, (Sept 11, 2018), http://www.finra.org/newsroom/2018/finra-charges-broker-fraud-and-unlawful-distribution-unregistered-cryptocurrency (last visited Sept 12, 2018). This case remains pending.

On Nov. 8, 2018, the SEC settled its first enforcement action against an unregistered cryptocurrency exchange. See Rachel Graf, SEC Puts Crypto Exchanges on Notice With First Settlement, (Nov. 8, 2018, 6:35 PM), https://www.law360.com/articles/1100245/sec-puts-crypto-exchanges-on-notice-with-first-settlement (last visited Dec. 9, 2018). The cryptocurrency exchange EtherDelta was found to be violating federal securities laws by trading assets that were considered securities without registering with the SEC first. EtherDelta's founder agreed to pay a $75,000 fine and $313,000 in disgorgement and interest but did not admit to any wrongdoing. This action by the SEC made clear that if digital tokens are considered securities during their initial sale, they may remain securities during subsequent trades.

May 2019 Update: On April 18, 2019, FinCEN announced a civil money penalty against a P2P virtual currency exchange for the first time. See, In a First, FinCEN Assesses Civil Money Penalty Against Peer-to-Peer Virtual Currency Exchanger, (April 26, 2019), https://www.jdsupra.com/legalnews/in-a-first-fincen-assesses-civil-money-25815/ (last visited May 27, 2019). FinCEN issued a press release announcing the penalty for violations of the BSA AML compliance program by an individual who acted as a P2P currency exchanger. This enforcement action is the first of its kind by FinCEN. According to FinCEN, the individual conducted transactions as a money transmitter. In particular, FinCEN found the individual purchased and sold virtual currency to others and completed sales and purchases by physically delivering or receiving currency in person, sending or receiving currency through mail, or in coordinated transactions by wire. FinCEN alleged that the activities were done in violation of BSA's money service business registration, AML compliance program and reporting requirements. The individual was assessed a $35,000 penalty.

B. State Enforcement Trends

On May 21, 2018, the North American Securities Administrators Association (NASAA) launched "Operation Cryptosweep," the largest coordinated series of securities enforcement actions by U.S. and Canadian state regulators ever brought. To date, it has resulted in at least 200 inquiries and investigations and 35 pending or completed enforcement actions related to ICOs or cryptocurrencies since the beginning of May. See Regulators Crack Down on Crypto Scams Via 'Operation Crypto-Sweep', Fortune.com (May 21, 2018), http://fortune.com/2018/05/21/regulators-cryptocurrency-ico-scams/ (last visited May 30, 2018); see also Kate Rooney, State regulators expand 'Operation Cryptosweep' to 200 initial coin offerings, CNBC.com (Aug. 28, 2018), https://www.cnbc.com/2018/08/28/state-regulators-expand-operation-crypto-sweep-to-200-initial-coin-offeringinvestigations.html (last visited Sept. 10, 2018). The probe targets unregistered securities offerings promising lucrative returns without adequately advising investors of the risks, including suspicious cryptocurrency transactions and ICOs. The NASAA has also agreed to share information with the CFTC, which could serve as a basis for the federal authorities to bring their own enforcement actions.

As virtual currency and ICO regulations lag behind the growing popularity of this emerging technology, state regulators are stepping up their enforcement efforts. For example, on March 27, 2018, Massachusetts stopped five unregistered ICOs, even though there was no allegation of fraud. Texas has emerged as an early leader in "Operation Cryptosweep" and has cracked down on bitcoin mining farms who are operating in violation of state securities laws. New York has also stepped up its efforts to protect NY residents investing in cryptocurrencies and ICOs. On Feb. 7, 2018, the New York Department of Financial Services (NYS DFS) issued new guidance to virtual currency business entities to ensure they have comprehensive policies on preventing and reporting fraud.

On Apr. 17, 2018, the New York Office of Attorney General launched the "Virtual Markets Integrity Initiative," which requested a wide range of information from thirteen major virtual currency exchanges. Three of the four exchanges who declined to participate were referred to NYS DFS for further investigation. See https://virtualmarkets.ag.ny.gov/#key-findings (last visited Dec. 21, 2018). This heightened scrutiny is intended to inform enforcement agencies, investors, and consumers on virtual currency practices and is sending a strong message to unlicensed ICOs and cryptocurrency exchanges seeking to enter the New York market that they must comply with state licensing requirements.

On Sept. 18, 2018, the New York Office of Attorney General published its Virtual Markets Integrity Initiative Report on cryptocurrency trading platforms and the vulnerability many have to market manipulation. See https://ag.ny.gov/

sites/default/files/vmii_report.pdf?mod=article_inline (last visited Dec. 9, 2018). The report described issues with certain practices put in place by the exchanges, including methods for monitoring and preventing market manipulation. The report stated that serious market surveillance measures had not been taken by the industry to detect and punish suspicious trading activity and noted the industry could not take proper action to protect customers if it was not even aware of the practices in the first place. However, the report noted that most exchanges use KYC procedures already.

FUTURE REGULATORY TRENDS

So what to expect in the future? It is safe to say, as more regulators continue to weigh in on ICOs and virtual currencies, more regulation and enforcement is expected. In 2014, a Chamber of Digital Commerce was founded, and 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.

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, virtual currencies and blockchain transactions, managing AML, fraud and cybersecurity risks will remain top-of-mind for fintech companies seeking to gain investor confidence and will also 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.

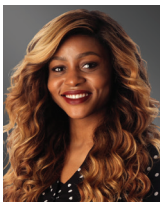
This article first appeared in Westlaw's publication entitled Payment Systems and Electronic Fund Transfers Guide. The publication is part of the Emerging Areas of Practice Series – a new publishing initiative which reduces product to market time to cover emerging areas of the law as they develop. New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

ABOUT THE AUTHOR

Obiamaka P. Madubuko is a Litigation and Compliance Shareholder at Greenberg Traurig and is based in the firm's New York office. Obi 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 Bank Secrecy Act (BSA), Foreign Corrupt Practices Act (FCPA), the Dodd-Frank Act, Office of Foreign Asset Control (OFAC) and other global trade regulations, including cybersecurity defense, data privacy 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. Obi is a member of the firm's Blockchain and Fintech Taskforce and the Financial Regulatory & Compliance Group.

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.

ABOUT THE AUTHOR



Margaret Ukwu is an Intellectual Property Litigation Associate at Greenberg Traurig and is based in the firm's New York office. Margaret 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.

Footnotes

1

However, the national fintech charter option as announced on July 31, 2018 by the U.S. Department of the Treasury's Office of the Comptroller of the Currency ("OCC") provides crypto-exchanges and other fintech firms a way to possibly bypass state-by-state licensing laws. This move by the OCC will potentially allow online lenders, payments firms, and cryptocurrency ventures to operate without having to get individual state licenses or rely on a bank. See Policy Statement on Financial Technology Companies' Eligibility to Apply for National Bank Charters, (July 31, 2018),

https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-occ-policy-statement-fintech.pdf (last visited Sept 6, 2018).