TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Guidelines for Anti-Money Laundering Compliance and Combatting the Financing of Terrorism

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • SEPTEMBER 2019

CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world's largest trade association representing the blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

TOKEN ALLIANCE

The Token Alliance is an industry-led initiative of the Chamber of Digital Commerce, developed to be a key resource for the emerging industry surrounding the generation and distribution of tokens using blockchain technology. Comprised of more than 400 industry participants, the Alliance includes blockchain and token and legal experts, technologists, economists, former regulators, and practitioners from around the globe. The Token Alliance develops community-driven guidelines for the responsible development of tokens.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES & WORKING GROUPS

SMART CONTRACTS ALLIANCE

Promotes real-world application of smart contracts to enhance the way business is conducted.

GLOBAL BLOCKCHAIN FORUM

Working with the world's leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.

BLOCKCHAIN ALLIANCE

The public-private forum for the blockchain community and law enforcement to help combat criminal activity.

BLOCKCHAIN INTELLECTUAL PROPERTY COUNCIL

Balancing the protection of proprietary information with the openness necessary for innovation.

DIGITAL ASSETS ACCOUNTING CONSORTIUM

Developing accounting and reporting standards for digital assets and blockchain-based technologies.

STATE WORKING GROUP

Engaging with state and local governments on the regulation and implementation of blockchain technology.

CHAMBER OF DIGITAL COMMERCE CANADA

Promoting the acceptance and use of digital assets and blockchain-based technologies in Canada.

TABLE OF CONTENTS

I. ACKNOWLEDGMENTS

TOKEN ALLIANCE CO-CHAIRS

PAUL ATKINS

Chief Executive Officer, Patomak Global Partners
Non-Executive Chairman, BATS Global Markets, Inc. (2012-2015)
Commissioner, U.S. Securities and Exchange Commission (2002-2009)

JAMES NEWSOME, PH.D.

Founding Partner, Delta Strategy Group
President & CEO, New York Mercantile Exchange (2004-2008)
Chairman, U.S. Commodity Futures Trading Commission (2001-2004)
Commissioner, U.S. Commodity Futures Trading Commission (1998-2001)

TOKEN ALLIANCE LEADERSHIP COMMITTEE

The Chamber of Digital Commerce would like to recognize the following individuals for their thought leadership, contributions and support to the Token Alliance in the production of this report.

KEVIN BATTEH
Partner,
Delta Strategy Group

PERIANNE BORING
Founder and President,
Chamber of Digital Commerce

JOE CUTLER
Partner,
Perkins Coie LLP

DAX HANSEN
Partner,
Perkins Coie LLP

CHRIS HOUSSER
Co-Founder,
Polymath

JONATHAN JOHNSON
President,
Medici Ventures

AMY DAVINE KIM
Chief Policy Officer,
Chamber of Digital Commerce

KARI LARSEN
Partner,
Perkins Coie LLP

BRIAN LIO
Chief Executive Officer,
Smith + Crown

RUMI MORALES
Partner,
Outlier Ventures

MATTHEW ROSZAK
Chairman and Co-Founder,
Bloq

BILL SHIHARA
Chief Executive Officer,
Bittrex

JOSHUA STEIN
Chief Executive Officer,
Harbor

COLLEEN SULLIVAN
Chief Executive Officer,
CMT Digital

EXPERT CONTRIBUTORS

The Chamber of Digital Commerce would like to extend a special thank you to the following individuals for helping to lead the development of this report.

STEVE BUNNELL
O'Melveny & Myers LLP

JOE CUTLER
Perkins Coie LLP

KENDRA HAAR
Perkins Coie LLP

DAX HANSEN
Perkins Coie LLP

LAUREL LOOMIS RIMON
O'Melveny & Myers LLP

We would also like to thank the following individuals for their valuable contributions to the Token Alliance in the production of this report.

SAM BORO
Perkins Coie LLP

THOMAS BORREL
Polymath

PAUL BRIGNER
Chamber of Digital Commerce

GREG FAVITTA
CipherTrace

KEVIN FELDIS
Perkins Coie LLP

MICHELLE GITLITZ
Blank Rome

JOHN JEFFERIES
CipherTrace

OLGA MACK
Quantstamp

STEVEN MERRIMAN
Perkins Coie LLP

MICHAEL OU
CoolBitX Technology

DIVIJ PANDYA
Chamber of Digital Commerce

ARABY PATCH
Securitize

MICHAEL SELIG
Perkins Coie LLP

STEVEN SPRAGUE
Rivetz

DAWN TALBOTT
RiskSpan

SAM WYNER
KPMG LLP

II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics — from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law — law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC)-regulated products and services laws (so-called "utility tokens" and associated platforms). Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries — the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons. This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.

We are excited to introduce these guidelines for anti-money laundering compliance to complement our work involving tokens. They supplement our reports on securities and non-securities tokens as well as consumer protection. AML compliance has always been a focus of industry from even before the time that FinCEN published its original guidance on convertible virtual currencies in 2013 and continues to be

a primary focus today. The latest approval by the FATF of Recommendations involving virtual assets and virtual asset service providers and FinCEN's most recent guidance for virtual currency businesses keep these issues at the forefront. We look forward to serving as a resource on this issue as technology, and criminal creativity, evolves.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE

- Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.
- This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that activities involving tokens will fully comply with the laws discussed herein.
- These views are being offered for discussion purposes only, and they have not been sanctioned by any regulator or government agency.

CONSULT LEGAL COUNSEL BEFORE ENGAGING IN ACTIVITIES INVOLVING DIGITAL TOKENS

- Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token, as well as companies engaging in holding or transferring digital tokens on behalf of others should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.
- Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.
- This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.
- Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.

III. CONSIDERATIONS AND GUIDELINES FOR ANTI-MONEY LAUNDERING COMPLIANCE

I. INTRODUCTION

This report provides an overview of laws in the United States aimed at the prevention of money laundering and at combatting the financing of terrorists ("CFT"), as well as the rules and regulations that certain categories of businesses must follow with respect to establishing formal anti-money laundering ("AML") policies and practices. It concludes with a set of guidelines for token sponsors and token trading platforms to consider when crafting AML and CFT compliance programs.

II. CRIMINAL AND CIVIL ANTI-MONEY LAUNDERING LAWS

A. CRIMINAL ANTI-MONEY LAUNDERING LAWS

Any person or business conducting a financial transaction that occurs wholly or partially in the United States is obligated under the criminal laws[1] of the United States to avoid transacting in criminal proceeds. The term "financial transaction" under these statutes is expansive, including transactions as varied as money transfers, currency exchange, loans, use of a safe deposit box, or gifts of tangible property.[2] The following types of financial transactions are subject to criminal prosecution:

- *Concealment or Promotion of Money Laundering,* 18 U.S.C. § 1956(a)(1): This statute prohibits a transaction in which a person knows that the property involved in a transaction constitutes the proceeds of some form of unlawful activity, even if that person does not know the precise nature of the underlying criminal activity.[3] To be in violation of this law, there must be an intent on the part of the person conducting the transaction — most often proven through circumstantial evidence — to conceal the true nature, location, source, ownership, or control of the funds, or to reinvest in or "promote" future criminal activity.
- *International Money Laundering,* 18 U.S.C. § 1956(a)(2): This law applies even to "clean" funds that are not currently the proceeds of criminal activity but are sent to or from the United States to "promote" certain categories of criminal activity.

1 A civil suit seeking a monetary penalty may also be brought for violations of 18 U.S.C. § 1956 pursuant to subsection (b).
2 18 U.S.C. § 1956(c)(3) and (4).
3 The property involved must, in fact, be the proceeds of one of a number of "specified unlawful activities" — a broad category including most profit-generating crimes.

- *Money Spending Statute,* 18 U.S.C. § 1957: This law prohibits transactions over $10,000 where the participant[4] knows the funds are derived from some unlawful source.[5]
- *Money Laundering Conspiracy,* 18 U.S.C. § 1956(h): Two or more individuals who intend to conduct a transaction in criminal proceeds may be liable for any foreseeable offenses committed by their co-conspirators in furtherance of the scheme.

For those individuals or businesses who are engaged in activity that may be considered money transmitting, another criminal statute, 18 U.S.C. § 1960, makes it unlawful to operate a money transmitting business without a state license if operating in a state where one is required, or without registering as a "money services business" with the Financial Crimes Enforcement Network ("FinCEN"). Additionally, section 1960 makes it a crime for a money transmitting business to transmit funds that are known to be criminal proceeds or intended to promote certain types of criminal activity. Importantly, a violation of this statute can occur even where the operators of the business did not know a state license was required.[6] Additionally, criminal liability under this statute applies broadly to anyone who knowingly "conducts, controls, manages, supervises, directs, or owns all or a part" of such an unlicensed money transmitting business.[7]

B. CIVIL ANTI-MONEY LAUNDERING LAWS

Although every business that conducts financial transactions should be aware of criminal AML statutes, certain types of businesses are subject to a broad range of AML requirements under the regulatory regime established by the Bank Secrecy Act ("BSA"), 31 U.S.C. § 5311 *et. seq*. The BSA applies to a variety of "financial institutions," which include banks, credit unions, securities broker-dealers, currency exchangers, check cashers, issuers, redeemers or cashiers of travelers checks, and money transmitters, among other entities.[8] As discussed more fully below, for financial institutions subject to its jurisdiction, the BSA establishes various recordkeeping requirements as well as reporting requirements related to transactions in currency and monetary instruments. Additionally, the BSA mandates that financial institutions provide timely and detailed reports to law enforcement of suspicious transactions that occur within a business's purview. Parties (individuals or businesses) that willfully violate the BSA are subject to criminal penalties.[9]

III. ECONOMIC SANCTIONS

U.S. persons must comply with U.S. sanctions law. The U.S. government uses economic sanctions to advance its foreign policy and national security goals. Various U.S. statutes and Executive Orders authorize the imposition of these sanctions. The Department of the Treasury's Office of Foreign Assets Control ("OFAC") has primary responsibility for administering sanctions programs. OFAC, in total,

4 The statute is applicable to transactions conducted by "financial institutions," which includes, among other things, a currency exchange, money transmitter, and a broker or dealer in securities or commodities. 18 U.S.C. § 1956(c)(6); 31 U.S.C. § 5312(a)(2).
5 Again, the funds must actually be derived from a "specified unlawful activity;" even if the person involved is not aware of which particular unlawful activity.
6 18 U.S.C. § 1960(b)(1)(A).
7 18 U.S.C. § 1960(a).
8 31 U.S.C. § 5312(a)(1)(2).
9 31 U.S.C. § 5322.

administers over two dozen active sanctions programs for two categories of sanctions. First, OFAC administers targeted sanctions against specific individuals and entities and, in some cases, specific vessels and aircraft. OFAC maintains a Specially Designated Nationals and Blocked Persons List ("SDN List") that identifies the specific individuals, entities, and properties subject to sanctions as well as other sanctions lists. Second, OFAC administers comprehensive sanctions programs against entire countries or regions. Currently, OFAC has comprehensive sanctions in place against Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine.

WHO IS COVERED

U.S. persons must comply with sanctions regulations, although the definition of U.S. persons varies by sanctions program. In general, the sanctions programs cover:

- Any person within the United States;
- U.S. citizens (including citizens living abroad);
- Legal permanent residents of the United States;
- U.S. companies; and
- Foreign branches of U.S. companies.

Some sanctions programs go farther and cover foreign entities "owned or controlled" by U.S. persons. But even if the specific program does not cover such entities (and, thus, the entity itself is outside the scope of the sanctions program), a U.S. entity controlling a foreign entity would still be obligated to comply with U.S. sanctions.

U.S. persons are generally prohibited from transacting directly with a Specifically Designated National ("SDN") or a party residing in a sanctioned region (collectively, a "blocked party"). Even if a specific entity is not on the SDN list, U.S. persons may still be prohibited from transacting with the entity if SDNs, in the aggregate, own 50% or more of the entity. Likewise, U.S. persons are generally prohibited from conducting a transaction that involves property in which a blocked party has an interest. If a U.S. person determines that it is holding a blocked party's property, the U.S. person must block further transactions and, within 10 days of the blocking, file a blocked property report with OFAC.

FACILITATION

Even if a U.S. person does not transact directly with a blocked party, U.S. persons also violate sanctions laws if they approve or facilitate a transaction that would be prohibited if U.S. persons conducted the transaction directly. For instance, a U.S. citizen controlling a foreign entity may violate U.S. sanctions laws if the U.S. citizen authorizes the company to conduct a transaction with a blocked party. Similarly, U.S. persons cannot engage in a transaction that evades the prohibitions within a particular sanctions program.

STRICT LIABILITY

Assignment of fault and potential penalties for violating OFAC's sanctions regulations follow a standard of "strict liability." That is, the sanctions regulations do not incorporate an intent or a knowledge component. If a U.S. person engaged in a prohibited transaction (or facilitated a prohibited transaction), a sanctions violation can occur even where the violation was unintentional, unknown, or did not result from negligence.

PENALTIES

U.S. persons should take great care to avoid sanctions violations because the penalties can be severe. Some sanctions programs carry civil penalties that can be greater than $250,000 per violation or twice the amount of the violating transaction. Criminal penalties also can apply for willful sanctions violations.

VIRTUAL CURRENCIES

OFAC has made clear, through a series of FAQs, that the compliance obligations are the same whether the transaction is in fiat dollars or virtual currency. OFAC expects that virtual currency businesses subject to OFAC's jurisdiction will develop compliance programs tailored to each business's individual risks and designed to prevent transactions involving blocked parties and property.

THE VENEZUELAN PETRO

Still, there are sanctions compliance wrinkles unique to virtual currency businesses. U.S. persons are prohibited from engaging in transactions that relate to Venezuela's Petro, a virtual currency issued by the Venezuelan government. On March 19, 2018, President Trump signed Executive Order 13827 prohibiting U.S. persons from providing financing for or dealing in any "digital currency, digital coin, or digital token" that was "issued by, for, or on behalf" of the Venezuelan government.

WALLET ADDRESSES

On November 28, 2018, OFAC announced that it was adding two virtual currency addresses to the SDN List of two SDNs. OFAC's addition of virtual currency addresses to the SDN List means that, in addition to using traditional identifiers to screen out blocked parties and property, virtual currency businesses must also screen for and block transactions that involve blockchain addresses identified by OFAC as being associated with SDNs.

IV. REGULATION AND ENFORCEMENT ON THE FEDERAL AND STATE LEVEL

A number of different agencies on both the federal and state level exercise AML rule making, oversight, and enforcement authority over businesses subject to their jurisdiction. Because of this, a digital currency business may be subject to the simultaneous jurisdiction of multiple state and federal authorities, depending on the nature of their activities. Although federal regulators are primarily focused on compliance with the BSA and utilize a mostly consistent body of rules and agency guidance across agencies, state regulators' primary focus is different. On the state level, regulation and enforcement arises out of a focus on consumer protection and, although state regulators do generally require and

examine a licensee's BSA/AML programs, state licensing regimes are aimed primarily at ensuring safety and soundness of the financial institution to ensure consumer protection.

A. FEDERAL

A number of different agencies on the federal level are responsible for monitoring and enforcing laws and regulations targeting money laundering and terrorist financing. Regulatory agencies conduct regular and routine examinations of the activities of financial institutions and may bring civil enforcement actions assessing monetary penalties either independent of, or concurrent with, criminal enforcement actions.

1. FINANCIAL CRIMES ENFORCEMENT NETWORK

FinCEN is an agency within the U.S. Department of Treasury's Office of Terrorism and Financial Intelligence whose mission is to "safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."[10] Although FinCEN has responsibility for ensuring businesses subject to its jurisdiction are in compliance with the BSA, it does not itself conduct examinations of those businesses.[11] Instead, examination authority for BSA compliance has been delegated to a number of other federal agencies and self-regulatory organizations. For example, depository institutions are examined by their own federal functional regulators (the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, etc.); securities broker-dealers are examined by the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"); and money services businesses are examined by the Internal Revenue Service ("IRS"). Nonetheless, relying upon the findings of an examination or other sources of investigation, FinCEN has independent authority to bring civil enforcement actions, including monetary penalties and other injunctive relief.

2. SECURITIES AND EXCHANGE COMMISSION AND FINANCIAL INDUSTRY REGULATORY AUTHORITY

Broker-dealers and other participants in the market for securities are regulated by the SEC and are subject to compliance with the BSA and its implementing regulations.[12] Additionally, FINRA, a non-governmental self-regulatory organization that operates under the SEC's oversight, develops and enforces AML rules that apply to the activities of all registered broker-dealer firms and registered brokers in the United States. Both the SEC and FINRA conduct regular examinations of the entities within their jurisdiction, and, in the last year, both have announced exam priorities focused on AML programs.[13] Both agencies also have the authority to bring civil enforcement actions related to AML failures, which have included both corporate and individual penalties.

10 Fin. Crimes Enf't Network, Mission, https://www.fincen.gov/about/mission (last visited Aug. 15, 2019).
11 Govt. Accountability Office, *Anti-Money Laundering: U.S. Effort to Combat Narcotics-Related Money Laundering in the Western Hemisphere,* (Aug. 2017), https://www.gao.gov/assets/690/686727.pdf.
12 *See* Sec. 17(a) of the Securities Exchange Act of 1934, Rule 17a-8.
13 Office of Compliance Inspections and Examinations, 2018 National Exam Program Examination Priorities, Sec. and Exchange Comm'n (Feb. 7, 2018), sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

3. COMMODITY FUTURES TRADING COMMISSION

The Commodity Futures Trading Commission ("CFTC") oversees individuals and organizations participating in derivatives markets and other products subject to the Commodity Exchange Act, including, among other things, swap execution facilities, derivatives clearing organizations, swap dealers, futures commission merchants, and commodity pool operators. The AML program requirements contained in the BSA and its regulations apply to futures commission merchants and introducing brokers regulated by the CFTC. The CFTC relies on the National Futures Association ("NFA"), the self-regulatory organization for the derivatives industry that it oversees, to establish and enforce rules implementing AML requirements for the NFA's registered members. The NFA conducts routine examinations of its members and brings enforcement actions that may include civil monetary penalties for violations of AML compliance rules.[14]

4. DEPARTMENT OF JUSTICE

The Department of Justice ("DOJ") has authority to investigate and prosecute criminal and civil enforcement actions related to violations of federal AML and CFT laws. Working with a number of federal investigatory agencies, including the Federal Bureau of Investigation, IRS, Drug Enforcement Administration, Homeland Security Investigation, and others, the DOJ conducts grand jury investigations and brings criminal and civil prosecutions of individuals and businesses under federal money laundering, money transmitting, and terrorist financing laws. Because money laundering is a criminal offense under various federal statutes, the DOJ's prosecutions can include and have included actions against financial institutions — and their compliance officers and executives — for violations of laws prohibiting money laundering and terrorist financing.[15] A prosecution may be brought by one of the 94 U.S. Attorney's Offices located throughout the country, or by an office within the DOJ headquarters in Washington, D.C., typically DOJ's Money Laundering and Asset Recovery Section ("MLARS"),[16] or jointly by both offices.

Unlike civil regulators that are charged with ensuring regulated entities maintain appropriate and effective AML programs, the DOJ is focused on prosecuting those entities and individuals who engage in or facilitate criminal money laundering or terrorist financing — including turning a blind eye to such activity taking place. The DOJ has a long history of pursuing criminal sanctions — imprisonment, fines, and forfeiture — against individuals and companies violating federal AML and CFT laws.

B. STATE

On the state level, financial activity affecting state residents is subject to oversight by both a state's financial regulators, a state's Attorney General, and other local law enforcement agencies.

---

14 Complaint, In the Matter of LBS Limited Partnership (NFA ID #245169), Nat'l Futures Ass'n (June 11, 2018), https://www.nfa.futures.org/basicnet/CaseDocument.aspx?seqnum=4558.

15 *See, e.g.,* DOJ, Banamex USA Non-Prosecution Agreement, Attachment A at 1 (May 18, 2017) (finding BSA violation where MSB failed to "provide appropriate staffing and resources to ensure its BSA department could conduct appropriate transaction monitoring").; *In the Matter of Ripple Labs* (DOJ May 5, 2018).

16 Dept. of Justice, *Money Laundering and Asset Recovery Section* (MLARS), https://www.justice.gov/criminal-mlars (last visited Oct. 19, 2018).

1. FINANCIAL REGULATORS

Almost all states in the United States regulate the transmission of money, and many states have robust licensing programs that require businesses to be licensed for that activity before engaging in any transactions with residents of a particular state. Across the United States, licensing regimes commonly include a registration requirement, the collection of biometric information for executives and other persons in "control," a surety bond, minimum capitalization requirements, and submission to regular state regulator examinations.[17] The onerousness of these requirements varies by state, as does the specificity of the agency guidance that can assist companies with navigating the requirements. Many states participate in the Conference of State Bank Supervisors ("CSBS"), a consortium of state banking regulators. CSBS oversees the National Multistate Licensing System ("NMLS"), which states increasingly use to process applications for money transmitter licenses.[18] CSBS also issues policies and reports that may influence state regulator action. The CSBS issued a model regulatory framework on September 15, 2015, that was designed to support the CSBS Policy on State Regulation of Virtual Currency and to promote consistent state regulation of virtual currency activities.[19]

In February 2018, seven states committed to a multi-state agreement ("Multistate Compact") that standardizes key elements of the licensing process for money services businesses.[20] For startups in the fintech and cryptocurrency industry, the requirement to obtain licenses in all states and territories that require it can be much more cumbersome than federal compliance — to the extent that it may have a chilling effect on innovation.[21] Through the Multistate Compact, regulators in Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington announced their agreement that if one state reviews key elements of state licensing for a money transmitter (*e.g.,* IT, cybersecurity, business plan, background check, and compliance with the BSA), then the other participating states agree to accept the findings. The plan is that this process will significantly streamline the application and review process for both regulatory agencies and applicants. The Multistate Compact is the first step among regulators to move towards an integrated, 50-state system of licensing and supervision of fintech companies. More detail on state licensing requirements is provided below.

State financial regulators, such as the Department of Financial Services in New York and the Department of Financial Institutions in Washington State, conduct regular examinations of money transmitter businesses and may bring regulatory enforcement actions involving monetary fines, suspension or revocation of licenses, or other injunctive relief.

17 Benjamin Lo, *Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation,* 18 Yale J. L. & Tech. 1 (2016).
18 Nat'l Multistate Licensing Sys., *Organizational Chart,* https://nationwidelicensingsystem.org/about/Pages/OrgChart.aspx (last visited Oct. 19, 2018).
19 *Model Regulatory Framework for Virtual Currencies,* CSBS (Mar. 30, 2017), https://www.csbs.org/model-regulatory-framework-virtual-currencies; State Regulatory Requirements for Virtual Currency Activities CSBS Model Regulatory Framework, CSBS (Sept. 15, 2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.
20 State Regulatory Requirements For Virtual Currency Activities CSBS Model Regulatory Framework, CSBS (Sept. 15, 2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.
21 Tim Fernholz, *The Patchwork of Regulations Entangling Square, and Every American Internet Startup That Takes Money,* Quartz (Mar. 14, 2013), https://qz.com/62265/why-square-and-seven-other-finance-start-ups-got-run-out-of-illinois/.

2. STATE ATTORNEYS GENERAL AND LOCAL PROSECUTORS

State Attorneys General are empowered to investigate and bring suit against individuals and financial institutions that violate the state's laws and regulations. While state Attorneys General offices vary in terms of the scope of their criminal enforcement authority, individuals or businesses that engage in money laundering activity may be subject to either criminal or civil penalties pursuant to money laundering laws or to other statutes involving fraud, tax, or consumer protection.[22] Local district attorneys' offices also have jurisdiction to bring criminal prosecutions for money laundering violations under local and state laws.

V. ACTIVITY THAT IS SUBJECT TO REGULATION

For businesses that are engaging in financial services of any kind, a key threshold question is whether these activities are of the nature that they are subject to regulation by a federal or state agency such that they require the development of a comprehensive AML Compliance program. Businesses that, for example, offer cryptocurrency exchange services, issue their own tokens, provide lending services, operate a futures trading platform, or offer or provide blockchain-based non-financial services, will all require different analyses. Some aspects of a blockchain business's business model may be regulated by multiple regulators while other parts of the business model may not be subject to any regulation. Conduct involving cryptocurrency generally falls into one of four buckets of transactions: (i) direct purchases (*i.e.*, exchanging tokens for fiat currency); (ii) direct sales (*i.e.*, exchanging tokens for tokens); (iii) custodial wallets (*i.e.*, the service of holding the private key for the individual owner, thereby holding the value contained within that key on behalf of the owner); and (iv) facilitating trades between users (*i.e.*, the trade of one token for another token). Identifying the specific regulated activity is key to determining the proper scope of the corresponding AML Compliance program that must be developed and enacted by the business. There is no one-size-fits-all AML Compliance program. All programs need to be designed to address the specific nature of the business's services offered and the risk factors associated with those services and potential customer base.

A. FEDERAL MONEY TRANSMITTING

First, if a business is engaged in "money transmitting," which is a form of regulated "money services business" ("MSB") activity under the BSA, it is considered a "financial institution" under the BSA. A person or entity is a "money transmitter" when they

1. accept "currency, funds or other value that substitutes for currency from one person" and transmit "currency, funds, or other value that substitutes for currency to another location or person by any means" or
2. are "engaged in the transfer of funds."[23]

---

22 *See e.g.,* Iowa Dept. of Justice, *Western Union to Enhance Anti-Wire Fraud Program and Pay $5 Million through 49-State Consumer Fraud Agreement,* (Jan. 31, 2017), https://www.iowaattorneygeneral.gov/newsroom/western-union-to-enhance-anti-wire-fraud-program-and-pay-5-million-through-49-state-consumer-fraud/; Western Union, *Arizona Attorney General's News Release on Multi-State Settlement,* (Feb. 11, 2010), http://ir.westernunion.com/news/archived-press-releases/press-release-details/2010/Arizona-Attorney-Generals-News-Release-on-Multi-State-Settlement/default.aspx.

23 31 C.F.R. § 1010.100(ff)(5).

MSBs must register with FinCEN and comply with various federal AML and know-your-customer requirements (commonly referred to as "KYC") as well as recordkeeping and reporting requirements. Further, operating as an unlicensed MSB may result in civil and potentially criminal penalties under federal law.

In 2013, FinCEN first issued interpretive guidance to address how its regulations apply to persons administering, exchanging, or using virtual currencies. FinCEN's guidance on virtual currencies ("Virtual Currency Guidance") interprets the money transmitter definition as encompassing products it refers to as "convertible virtual currency" and entities that are either "administrators" or "exchangers" of such virtual currency.[24]

In this guidance, FinCEN defines an "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[25] An "exchanger," on the other hand, is more broadly defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." The definition of "exchanger" is the key term for platforms that permit trades of virtual currency for other virtual currency.

Notably, the Virtual Currency Guidance further states that an administrator or exchanger that "buys or sells virtual currency for any reason is a money transmitter," unless an exemption applies.[26] Although there are reasonable bases for arguing that this language should be interpreted more narrowly, in light of underlying (and controlling) FinCEN regulations and subsequent FinCEN administrative rulings, it does tend to indicate FinCEN's general intention to broadly regulate virtual currency activity within its regulatory jurisdiction.

VIRTUAL CURRENCY (in contrast to "real currency")

A medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency; specifically, virtual currency lacks the status of legal tender in any jurisdiction.

FinCEN defines "virtual currency," in contrast to "real currency," as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency;" specifically, virtual currency lacks the status of legal tender in any jurisdiction. Since this time, FinCEN has issued additional guidance clarifying its stance on activities in this industry.

24 *See* Dep't of Treas., Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* FIN-2013-G001 (March 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf. (hereinafter "Virtual Currency Guidance").
25 *Id.* at 2.
26 *Id.* at 3.

The Virtual Currency Guidance is limited to "convertible" virtual currency, which means a virtual currency that has "an equivalent value in real currency, or acts as a substitute for real currency." The threshold question then, for an analysis of Exchanger or Administrator compliance responsibilities with respect to any given token issuer, will almost always be whether the token sold constitutes a "convertible" virtual currency. If not, the issuer or exchanger would not likely be considered an MSB because it is not issuing or exchanging convertible virtual currency.

On May 9, 2019, FinCEN issued guidance regarding the "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (the "2019 Guidance").[27] While the 2019 Guidance purports to "not establish any new regulatory expectations or requirements," it delves into a number of specific applications and uses of convertible virtual currencies, and the application of certain requirements under the BSA.

Specifically, it reaffirms the principle of a strong "culture of compliance" and the need for a risk assessment to tailor AML compliance programs to mitigate known risks. In addition, for the first time, FinCEN details its views on the applicability of the Funds Transfer Rule and Funds Travel Rule to convertible virtual currency transactions, finding that they do apply to transfers of convertible virtual currency between financial institutions.

The 2019 Guidance also describes the application of specific business models involving the transmission of convertible virtual currency:

P2P Exchanges — BSA typically will apply unless involves a natural person engaging on an infrequent basis and not for profit or gain.

Wallets —

- "Hosted" wallets — typically hold customer funds and thus are money transmitters.
- "Unhosted" wallets — typically considered a "user" and thus not a money transmitter.
- Multi-signature wallet providers — if provided in conjunction with a hosted wallet, may be a money transmitter; if provided for an unhosted wallet, likely not a money transmitter.

ATMs/Kiosks — an owner/operator who uses the terminal to receive Convertible Virtual Currency and transmit it is a money transmitter for both transactions (receiving and transmitting).

27 *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, Fin. Crimes Enf't Network (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models .

Decentralized Applications (DApps) — the 2019 Guidance simply says that, similar to kiosks, when DApps perform money transmission services, the BSA will apply to the DApps, the owners/operators of the DApp, or both.

Anonymity-Enhanced Transactions —

- Anonymizing services provider — if they accept and transmit value, they are a money transmitter; the provision of privacy mechansims does not change the analysis nor does it qualify for the "intergral" exception.
- Anonymizing software provider – not a money transmitter pursuant to the exemption for delivery, communication, or network services access used by a money transmitter to support money transmission services. Note the user of the software may be a money transmitter.
- Providers of anonymity-enhanced Convertible Virtual Currencies (privacy coins) — may be a money transmitter if it acts as an administrator of a centralized Convertible Virtual Currency system and issues Convertible Virtual Currency in exchange for payment; uses such Convertible Virtual Currency to pay for goods and services typically not money transmitters; develops of decentralized Convertible Virtual Currency payment systems if accepts and transmits value.
- Money transmitters that accept or transmit anonymity-enhanced Convertible Virtual Currencies — FinCEN notes that these organizations must comply with the Funds Travel Rule and determine the identity of transmittors or recipients.

Payment Processors — are money transmitters and not eligible for the payment processor exception.

Internet Casinos — if not considered a "casino" under the BSA, may still be considered a money transmitter.

Models That May Be Exempt —

- Trading Platforms and Decentralized Exchanges — may be exempt if the parties to the transaction settle the trade themselves (off the platform).
- Initial Coin Offerings.
  - At Issuance — generally the issuer acts as an administrator at the time of issuance. Nevertheless, exceptions may apply, including when: a) they are a bank or registered with, and functionally regulated or examined by, the SEC or CFTC, and b) the fundraising activity falls under the integral to the sale of goods and services exemption, unless the asset serves as value that substitutes for currency.
  - Purchase or Resale — Generally, resale by the investor does not create BSA obligations for the investor. (Note if SEC or CFTC jurisdiction applies, other requirements will be triggered.)
  - DApp Developer — Dapps financed through ICO fundraising activity consists of the production of goods and services and is not money transmission. If deployed to engage in money transmission, then will qualify as a money transmitter.
  - DApp User — if deployed to engage in money transmission, then will qualify as a money transmitter.
  - Pre-mining — if used to pay for goods and services, or repay obligations (such as amounts owed to project investors), then not money transmission.
- Mining Pools — typically not money transmitters but will be if host a wallet on behalf of pool members or contract purchasers.

The list represents a summary of the 2019 Guidance. If you have a particular use case that falls within one of the above categories, please consult the Guidance directly.

If you are selling a token, issuing a token, or exchanging tokens for cryptocurrency or fiat currency, it is advisable to consult counsel to evaluate your particular services and payment flows, and help determine if your organization should register with FinCEN.

B. STATE MONEY TRANSMITTING

1. WHAT STATES GENERALLY REGULATE

States regulate a broad range of conduct under money transmitter laws. The traditional conduct known as “money transmission” accepts currency, funds, or value from one person in order to transmit that value to another location or person by any means. State laws on money transmission vary widely but can generally be grouped into several categories. Most states define money

transmission as including some or all of three types of activities: (1) the receipt of money or monetary value for transmission, (2) issuing and/or selling payment instruments, and (3) issuing and/or selling stored value. Currently, 49 states plus the District of Columbia regulate money transmission. Many of these states only regulate these activities when "money" is involved, which is generally defined as "a medium of exchange that is authorized or adopted by a domestic or foreign government."[28] State statutes with this limitation will not, by their own terms, govern activities involving virtual currencies exclusively, which are not adopted by any domestic or foreign government.[29]

Some states have taken a position that the state will not regulate transactions involving cryptocurrencies or digital assets. Other states' money transmitter laws define "currency" to only include government-backed monetary value (or fiat currency). Some state money transmitter statutory schemes have broader definitions of "currency" that would include value represented by cryptocurrency or digital assets. Finally, some states have adopted legislation or have taken positions directly addressing how cryptocurrency, virtual currency, digital currency, or digital assets will be treated in that state.[30]

Some states have promulgated exceptions to their money transmitter licensing laws and regulations that, if applicable to a particular company, can ease the burdens of complying with the patchwork of existing state money transmitter laws. However, the substantial variation in how states have interpreted and applied their exceptions means that a careful state survey is prudent before a company determines that it will not register as a money transmitter if it conducts these activities in a particular state.

If you are selling, storing, or trading a token, especially if the token functions as a means of moving monetary value, you will likely need to be licensed to operate in the various states, and you should analyze your business model and payment flows on a state-by-state basis. Please consult an attorney to review the flow of funds for your particular operation in order to determine where you need to apply for licensure.

2. STATE LICENSING (CONSUMER PROTECTION) VS. FEDERAL REGISTRATION

Money transmission is regulated at both the federal and state levels, but for different reasons, and with a different focus. Federal registration with FinCEN is focused on combatting money laundering efforts throughout the world. To register with FinCEN, your organization must have an

28 Note that Oregon is an exception — defining "money" as "a medium of exchange that: (a) The United States or a foreign government authorizes or adopts; or (b) Represents value that substitutes for currency but that does not benefit from government regulation requiring acceptance of the medium of exchange as legal tender." Or. Rev. Stat. § 717.200.

29 *See, e.g.,* Texas Dept. of Banking, *Supervisory Memo. - 1037* (updated Jan. 2, 2019), https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (noting that "[b]ecause neither centralized virtual currencies nor cyptocurrencies are coin and paper money issued by the government of a country, they cannot be considered currencies under the statute. Therefore, absent a legislative change to the statute, no currency exchange license is required in Texas to conduct any type of transaction exchanging virtual with sovereign currencies."). Texas' guidance provides a similar analysis regarding money transmission ("Because cryptocurrency is not money under the Money Services Act, receiving it in exchange for a promise to make it available at a later time or different location is not money transmission."). Under this guidance, the analysis may change when a cryptocurrency transaction involves sovereign (fiat) currency.

30 States that have directly addressed how the state will handle cryptocurrencies (either by statutory amendment or formal guidance) include: Alabama, Colorado, Connecticut, Georgia, Illinois, Kansas, New Hampshire, New Mexico, New York, North Carolina, Pennsylvania, South Carolina, Tennessee, Texas, Washington, and Vermont.

AML compliance program and processes in place to catch suspicious activities that may be related to money laundering.

In contrast to federal requirements, the 50-state money transmitter licensing regime is aimed more at consumer protection by making sure that companies who receive funds from consumers protect, store, and transmit those funds safely, securely, and accurately. That said, all states also view their licensing oversight as complimentary to and supportive of federal AML goals; and some states even have integrated AML compliance obligations into their money transmission licensure requirements.

The application process to obtain a money transmitter license in each state is far more onerous than registering with FinCEN. States look into the company's finances (including historical finance report), litigation history, criminal history, bankruptcy history, employment history of controlling persons, among a plethora of other information.

C. SECURITIES OR COMMODITIES

Although SEC officials have stated that some cryptocurrencies such as bitcoin and ether are not securities subject to SEC oversight, it does assert jurisdiction over most, if not all, ICOs which it believes are methods to raise capital by issuing securities that must be registered unless an exemption to the registration requirement applies.[31] A determination of whether a token or coin is a security depends on an application of the *Howey* Test.[32] Pointing to *Howey*, the SEC has stated that, to the extent a token or coin is offered or sold in a way that causes investors to have a reasonable expectation of profits based on the efforts of others, it is a security; and it sees most token or coin sales as fitting that description.[33] Consistent with this position, the SEC has brought enforcement actions aimed at enforcing registration requirements for securities related to ICOs.[34] Similarly, while the CFTC generally recognizes the SEC's jurisdiction over ICOs, it asserts its own jurisdiction over virtual currency derivatives and in instances where there is fraud of manipulation involving virtual currency markets.

It is worth noting that FinCEN regulations specifically provide that businesses "registered with, and functionally regulated or examined by" either the SEC or CFTC are excluded from the class of "money services businesses" that are regulated by FinCEN. (Such organizations will be subject to the AML requirements of the SEC or CFTC.) However, in practice, there currently exists a substantial lack of clarity about what the lanes of each of the federal regulators are and whether there will continue to be overlapping assertions of jurisdiction.

1. AML REQUIREMENTS APPLICABLE TO REGULATED BLOCKCHAIN COMPANIES

A business that is conducting activity that is regulated by any federal regulator must develop and maintain an AML program that meets the same general criteria. Most broadly, businesses that

31 Spotlight on Initial Coin Offerings (ICOs) , Sec. and Exchange Comm'n, https://www.sec.gov/ICO (last visited Aug. 15, 2019).
32 *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
33 William Hinman, Digital Asset Transactions: When Howey Met Gary (Plastic), Remarks at the Yahoo! Finance All Markets Summit: Crypto (June 14, 2018), The DAO, Exchange Act Release No. 81207 (July 25, 2017), https://www.sec.gov./litigation/investreport/34-81207.pdf .
34 SEC Annual Report, Division of Enforcement, 7. https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

are subject to the regulatory requirements discussed above are required to develop, implement, and maintain an effective anti-money laundering program reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.[35]

Those businesses that engage in money transmitting or other money services under federal law are required to register with FinCEN, which involves the submission of an electronic form on FinCEN's website[36] to provide information about the business, including: identification of the business's owner or controlling person, type of money services being provided, location of business, and bank account information for the business's primary transaction account.

To meet AML requirements, a business must have a formal AML compliance program that includes the following four elements: 1) written policies and procedures; 2) a designated AML compliance officer; 3) independent review and monitoring of the AML program, and 4) a training program for relevant personnel regarding their AML responsibilities. Additionally, money services businesses are subject to a number of reporting and record-keeping requirements, particularly, the requirement to file Suspicious Activity Reports, or "SARs", for transactions over $2,000 that appear to involve funds from illicit activity, be designed to evade reporting requirements under the BSA, or serve no apparent lawful or business purpose.

Although it may be possible to assign the responsibilities for your AML compliance program to a founder, manager, or employee with other duties if your business does not currently support a stand-alone function, keep in mind that it is critical that this function be resourced and, most importantly, free from the influence of the business or sales side of the organization.

Many participants in the cryptocurrency and token sale marketplace are based outside of the United States. If a company has what FinCEN refers to as foreign "agents," a term it uses to include "authorized delegates, foreign agents or counterparties, agents, and sub-agents," the business' AML program must meet additional requirements. For example, if there is a contractual arrangement to make tokens available to a foreign company or its customers through the foreign company's software platform, you must:

- conduct due diligence on foreign agents and counterparties;
- consider a number of particular risk factors and conduct risk-based monitoring of your agents and counterparties, and;
- develop and implement a policy for corrective action and termination for non-compliant entities.

35 31 C.F.R. § 1022.210.
36 Money Services Business (MSB) Registration, Fin. Crimes Enf't Network, https://www.fincen.gov/money-services-business-msb-registration (last visited Aug. 15, 2019).

VI. GUIDELINES BASED ON LESSONS FROM ENFORCEMENT, EXPERIENCE WITH REGULATORS, AND BEST PRACTICES

Blockchain and virtual currency companies are no longer completely novel. State and federal regulators have started issuing guidance, bringing enforcement actions, and amending their statutes and regulations to address it. The following section provides some high-level guidelines for token issuers and operators of businesses that trigger AML laws and regulations and need to demonstrate appropriately calibrated compliance.

A. CREATE A STRONG CULTURE OF COMPLIANCE WITH A SUPPORTIVE TONE FROM THE TOP

FinCEN's guidance emphasizes the importance of a culture of compliance.[37] The agency's view is that "[r]egardless of its size and business model, a financial institution with a poor culture of compliance is likely to have shortcomings in its BSA/AML program."[38] To this end, the agency recommends active engagement at a company's leadership and board levels, and makes clear that "[t]he commitment of an organization's leaders should be visible within the organization, as such commitment influences the attitudes of others within the organization."[39] Consistent with these principles, the agency has initiated enforcement actions against financial institutions that fail to promote effective information sharing between the company's AML Officer and its leadership.[40]

B. DEVELOP A COMPREHENSIVE COMPLIANCE PROGRAM

Any entity that registers as an MSB with FinCEN, applies for state money transmitter licenses, or identifies a need to implement AML compliance procedures should identify and designate a BSA/Compliance Officer early in the business's development stage. This role can be filled initially by someone with other duties but will ultimately need to be undertaken by someone with experience and knowledge of AML rules and regulations. An effective compliance program is based on a comprehensive assessment of relevant risks and tailored to mitigate or eliminate those risks. Third-party service providers who help perform AML or other compliance functions (like OFAC screening services and identity verification providers) should be clearly and intentionally integrated into the compliance program and service providers should perform their services free from undue influence from the business, marketing, or sales sides of the organization (who may encourage cutting corners on KYC to improve onboarding and customer retention metrics). These third parties should be carefully vetted to ensure that they reliably perform their advertised services. You should audit that compliance early and often.

37 FinCEN, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, FIN-2014-A007 (Aug. 11, 2014).
38 *Id.*
39 *Id.*
40 *See, e.g., In the Matter of First Bank of Delaware,* No. 2012-01 (Nov. 19, 2012) (explaining that "the Bank's Board and other appropriate Bank personnel were not notified of numerous instances of potential suspicious activity" related to the MSB business line, and that "the BSA Officer failed to escalate BSA problems to senior management").

C. EMPOWER THE AML/COMPLIANCE OFFICER WITH RESOURCES AND AUTHORITY TO REMEDY PROBLEMS

FinCEN has also made clear the importance of granting the AML Officer sufficient resources and authority to effectively monitor the AML risks present in a company's business model, as well as adequate authority to ensure any deficiencies are promptly redressed.[41] This is critical because "[t]he failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures" — such as the inability to monitor transactions and accounts or to ensure timely filing of SARs.[42] Again, FinCEN has supported this guidance with enforcement actions that target companies with insufficiently resourced and staffed AML programs.[43]

D. ENABLE FLOW OF REPORTING BETWEEN BUSINESS UNITS AND AML OFFICER

FinCEN's guidance specifically criticizes companies that fail to adequately share information between their AML departments and other relevant units within the business.[44] In 2014, FinCEN noted a troubling trend in information silos within organizations that ultimately precluded AML departments from obtaining sufficient information to effectively carry out their BSA responsibilities. Again, in this space, FinCEN's warnings have been preceded and followed by enforcement actions targeting companies that have inadequately developed reporting processes by which relevant information can flow between the AML Officer and the business.[45]

E. CONDUCT EFFECTIVE CUSTOMER ONBOARDING/KYC

The regulations governing MSBs require them to implement written AML compliance programs that incorporate policies and procedures reasonably designed to effectively "verify" customers' identification.[46] The extent and thoroughness of the verification requirement is not specified in the MSB regulations. That said, an entity's procedures must be appropriately tailored to the money laundering risk associated with the platform, the customer, and the transaction.

It is generally viewed as insufficient to collect only the name and email address of a customer. Further, entities should request the name and physical address of a customer and confirm such information by viewing an appropriate and valid identification document. Entities should establish systems (whether manual, automated, or both) to verify that all required identification data fields are completed and

41 FinCEN, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, FIN-2014-A007 (Aug. 11, 2014).
42 *Id.*
43 *In the Matter of: U.S. National Bank Association*, No. 2018-01 (FinCEN Feb. 15, 2018) ("Appointing a BSA officer is not sufficient to meet the regulatory requirement if that person does not have sufficient authority, resources, or time to satisfactorily complete the job."); Deferred Prosecution Agreement Statement of Facts, *U.S. v. HSBC Bank USA, N.A.*, 1:12-cr-00763-ILG (E.D.N.Y. Dec. 11, 2012) (ECF No. 3-3) (faulting HSBC for combining the roles of General Counsel and AML Compliance Officer).
44 Fin. Crimes. Enf't Network, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance,* FIN-2014-A007 (Aug. 11, 2014) ("Several recent enforcement actions noted that the subject institution had relevant information in its possession that was not made available to BSA/AML compliance staff. This may have resulted from a lack of an appropriate mechanism for sharing information, a lack of appreciation of the significance or relevance of the information to BSA/AML compliance or an intentional decision to prevent compliance officers or staff from having access to the information.")
45 *In the Matter of Oppenheimer,* No. 2015-01 (Jan. 26, 2015) ("[Di]vision of responsibility [between the AML Group and Surveillance Group] and the resultant silos of information contributed to the Firm's failure to identify and investigate the suspicious . . . activity at issue in this matter."); *In the Matter of Thomas Haider*, No. 2014-08 (Dec. 18, 2014) ("This arrangement — maintaining separate 'silos' of information within [MSB's] various departments such that [its] SAR analysts did not possess relevant information — was in place throughout [the CCO]'s employment."); *In the Matter of American Express Bank Int'l,* No. 2007-01 (Aug. 3, 2007) (explaining compliance responsibilities were insufficiently defined and implemented with respect to "escalating or sharing identified negative customer information among appropriate personnel at the Bank.").
46 *See* 31 C.F.R. § 1022.210(d)(1)(i)(A).

that false names (such as Donald Duck or Satoshi Nakamoto) are captured and reviewed. In such instances, the entity should have procedures in place that designate the required information and documentation to be provided and steps to take to determine whether to deny the application or shut the account, as appropriate.

When dealing with non-natural persons, such as legal entities, MSBs should develop appropriate customer onboarding procedures to vet and verify corporate records necessary to validate prospective corporate or enterprise customers. For example, MSBs should require identification documentation to confirm the identities of the ultimate beneficial owners of the company. They should also request corporate articles of incorporation, bylaws, and lists of Board members. Care should be taken to understand the ultimate source of funds for corporate or enterprise customers and to ensure that the company is not unwittingly allowing illicit funds to pass through its platform under the guise of corporate or wholesale transactions.

Finally, entities should devise and frequently test their verification procedures to ensure they are reliable and effective and make corrections or updates where needed.

F. CONDUCT VIGILANT TRANSACTION MONITORING AND SAR FILING

FinCEN has initiated a significant number of enforcement actions upon determination that a company failed to adequately monitor transactions for suspicious activity,[47] and in turn failed to timely file SARs as required by the BSA and its implementing regulations.[48]

Not only are the above offenses subject to criminal or civil prosecution, but the proceeds of criminal activity, and any property "involved" in a money laundering offense that may include such things as non-tainted funds in the same account, commissions or fees, websites, or even an entire business, are subject to criminal or civil forfeiture.

State regulators, New York in particular, are increasingly insistent that licensees involved in the blockchain space develop and maintain processes and procedures to effectively monitor transactions to identify, prevent, and report suspicious activity. These obligations, while not required by any specific statutory requirement, can be imposed in supervisory agreements or additional guidance.

Transaction monitoring should be a mixture of automated and manual processes, tailored to individual circumstances, but aimed at effective identification and prevention of use of the services to launder money or commit or facilitate crime. As with the use of third-party service providers for other aspects

47 *In re King Mail & Wireless, Inc.*, No. 2015-06 (June 1, 2015) (finding the MSB liable for failing to report "multiple wire transfers that were conducted on the same day, or within a few days of each other, and in amounts that [individually] would not trigger the recordkeeping requirements"); *In re Gibraltar Private Bank & Tr.*, No. 2016-01 (Feb. 25, 2016) (finding bank liable for a "transaction monitoring system contain[ing] account opening information and customer risk profiles that were frequently incomplete, inaccurate, and lacked sufficient analysis and validation").

48 *In re U.S. Bank,* No. 2018-01, (Feb. 15, 2018) (finding bank liable for "capping the number of alerts its automated transaction monitoring system would generate for investigation . . . caus[ing] the Bank to fail to investigate and report large numbers of suspicious transactions"); *In the Matter of W. Union Fin. Servs.*, No. 2017-01 (Jan. 19, 2017) (finding an MSB liable for taking "over 90 days to investigate activity for which it had facts to constitute the basis for filing a SAR"); *First Nat'l Cmty. Bank,* No. 2015-03, at 3-4 (Feb. 27, 2015) (failure to file SARs for activity related to a subpoena about a certain customer "deprived law enforcement of information that may have assisted law enforcement in tracking millions of dollars in related corrupt funds"); *In re Haider*, No. 2014-08 (Dec. 18, 2014) (finding that "individuals responsible for filing SARs were not provided with information possessed by [the company's] Fraud Department that should have resulted in the filing of SARs").

of compliance, entities should take great care not to rely solely on third parties for transaction monitoring, as that responsibility lies primarily with the MSB or licensed money transmitter and cannot be fully outsourced.

G. CONDUCT APPROPRIATE SANCTIONS SCREENING

Even if the BSA is not triggered by your activities, OFAC sanctions prohibitions still apply. This means that you must know your counterparties to avoid inadvertently providing or facilitating the financing of terrorism or other sanctioned persons or entities. Screening activity should be tailored to the risk presented by your platform.

UNDERSTANDING DIGITAL TOKENS

Guidelines for Anti-Money Laundering Compliance and Combatting the Financing of Terrorism