Cannabis, crypto and broker-dealers in the anti-money laundering hot seat

LEXOLOGY® Webinars

CADWALADER

Speakers

Jodi Avergun

Todd Blanche

Joseph V Moreno

Christian Larson

LEXOLOGY® Webinars

CADWALADER

Jodi Avergun

Jodi Avergun is Chair of the firm's White Collar Defense and Investigations Group and a noted expert in anti-money laundering law and regulated substances. Her practice focuses on representing corporations and individuals in criminal and regulatory matters involving, among other things, anti-money laundering, the Foreign Corrupt Practices Act (FCPA), securities enforcement, healthcare, and general white collar matters.

She is the former Chief of the Narcotic and Dangerous Drug Section of DOJ's Criminal Division and the former Chief of Staff of the DEA. She is also a former federal prosecutor, having been an AUSA in the Eastern District of New York for more than a decade. She represents companies and individuals in cases involving both traditional and unusual applications of the Controlled Substances Act (CSA), and counts among her clients large and small wholesale distributors, manufacturers, retail chains, and pharmacists. She successfully represented the employees of FedEx in grand jury investigations and at trial, successfully represented the clubs of the NFL in CSA-related matters, and is the first independent reviewer appointed to oversee a CSA settlement. She also advises clients in the burgeoning legal cannabis space, particularly as it relates to banking and financial transactions. She has written and lectured widely on all aspects of controlled substance law, and is a regular speaker and commentator at business seminars and conferences. Jodi was selected to Global Investigation Review's Who's Who Legal: Investigations 2017, and was named a top 100 Women in Investigations in 2018 in the white-collar criminal defense area.

Todd Blanche

Todd Blanche is a partner in Cadwalader's global litigation group. His practice focuses on representing corporations and individuals in criminal and regulatory matters involving all types of white collar investigations, prosecutions and enforcement actions. He has successfully represented both companies and individuals facing grand jury subpoenas, criminal charges, regulatory inquiries and actions, and internal investigations. A former assistant US attorney for the Southern District of New York, he has extensive experience investigating all manner of white collar crime.

Joseph V. Moreno

Joseph Moreno, a former federal prosecutor, is a partner in Cadwalader's white collar defense and investigations group. Dual-qualified to practice in the United States and as a solicitor in England and Wales, he has extensive litigation and crisis management experience handling complex matters involving the US Department of Justice, the SEC, the US Department of Defense and other domestic and international regulators and law enforcement agencies. Representative matters have involved money laundering and terrorist financing, cybersecurity and data breach response, securities and accounting fraud, insider trading, the FCPA, the UK Bribery Act, and other criminal and civil matters.

Christian Larson

Christian Larson is an associate with Cadwalader's white collar defense and investigations practice in Washington DC. He has experience in a broad range of anti-money laundering and other white collar matters, including conducting investigations in response to government inquiries and designing policies and procedures to comply with complex regulations. Prior to joining Cadwalader, he worked with the International Monetary Fund, the Organization for Security and Co-operation in Europe (OSCE) and the US Department of Justice Asset Forfeiture and Money Laundering Section. He has written numerous articles on anti-money laundering controls and served as head of the OSCE delegation to the Financial Action Task Force.

Overview

Anti-money laundering ("AML") programs have faced a slew of regulatory and enforcement changes in the past 18 months, and new challenges are on the horizon.

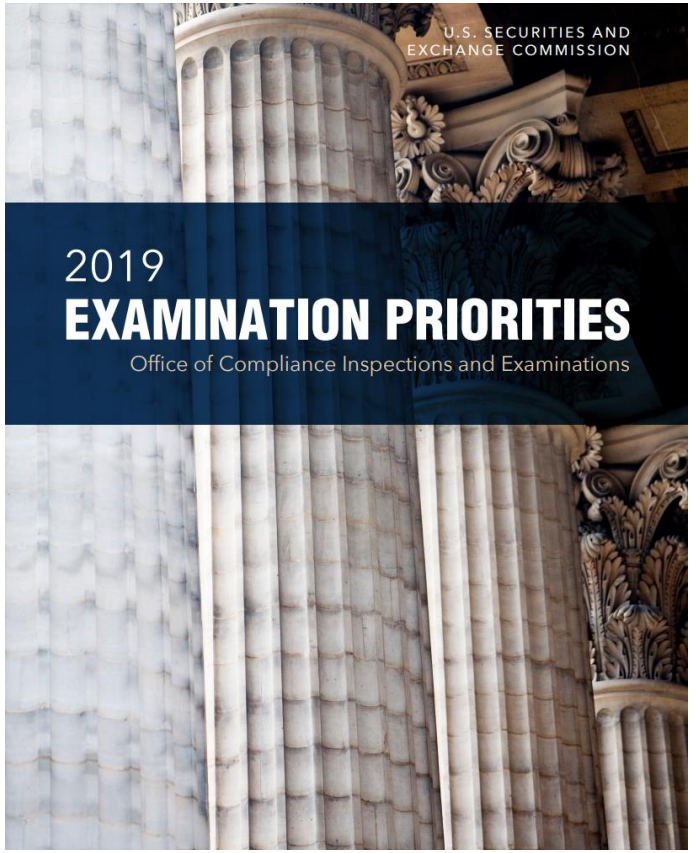
- This webinar will identify trends and lessons learned from the SEC and FINRA's enforcement focus on broker-dealer AML programs.
- In addition, the webinar will analyze the current state of play for financial institutions servicing cannabis businesses, including outcomes from recent Congressional debate on the issue.
- It will also evaluate the latest developments affecting the AML programs of businesses dealing with blockchain, cryptocurrency, or other digital assets.
- Finally, the webinar will provide an overview of expected changes to the Bank Secrecy Act and related regulations in 2019.

Broker-Dealer AML Programs

- SEC and FINRA Examination Priorities
- FINRA Examination Findings
- Enforcement Actions
- Takeaways

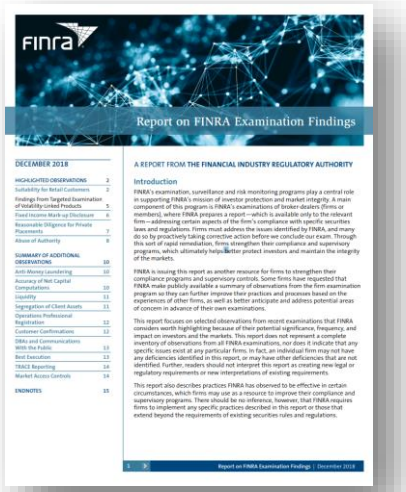
SEC and FINRA Enforcement Focus on Broker-Dealer AML Programs

- The SEC and FINRA published Examination Priorities for 2016, 2017, 2018 and 2019 included a focus on anti-money laundering programs
- Focus has been on three aspects of AML:
    1. Whether AML programs are tailored to the specific risks each firm faces
        - *E.g.* risks faced by introducing broker-dealers as opposed to clearing broker-dealers
    2. How broker-dealers are monitoring for suspicious activity at the firm; and
        - *E.g.* penny stock / microcap fraud
    3. Whether independent testing of the firm's AML program is effective.



SEC and FINRA AML Examination Findings

- The SEC's enforcement Annual Reports for 2016, 2017, and 2018 include no mention of anti-money laundering enforcement
- FINRA's Reports on Examination Findings include more feedback
- FINRA's published Examination Findings for 2017 identified five issues with broker-dealer AML programs:



1. Maintaining Adequate Policies and Procedures for Suspicious Activity

Some firms failed to establish and implement risk-based policies and procedures to detect and report suspicious transactions. FINRA identified these deficiencies where, for example, a firm's business growth far outpaced the growth of its AML programs, a portion of a firm's business involved a high-risk product (such as microcap securities or dual currency bonds), or a firm's business evolved over time and AML policies and procedures were not updated and adequately tailored to the firm's current risks, including with respect to how potentially suspicious activity would be monitored and documented.

2017 FINRA Published Examination Findings (cont'd)

2. Responsibility for AML Monitoring

While firms are permitted to delegate aspects of their suspicious activity monitoring program to non-AML staff (*e.g.*, to business line staff responsible for trade surveillance), in some cases where this was done, FINRA observed that problems sometimes arose with the appropriate and adequate escalation of potentially suspicious activity. Those problems typically occurred when the AML and surveillance staff did not share a common understanding of the types of activities that merited escalation or when staff did not escalate such activities appropriately. In some cases, the problems occurred because firms did not: (1) clearly define the activities that were being delegated; (2) articulate those delegations and related surveillance responsibilities in their written supervisory procedures; or (3) adequately train non-AML staff on AML surveillance policies and procedures.

3. Exclusions From Data Feeds Used for AML Monitoring

FINRA also observed instances where firms' monitoring systems were deficient due to gaps in the data feeding those systems that were created, for example, by the use of "suspense accounts" to process foreign currency money movement and conversion. The use of suspense and other operational accounts sometimes obscured the source of funds to firms' surveillance systems, resulting in weaker monitoring of high-risk transactions. FINRA also observed instances where firms made decisions to exclude certain types of customer accounts from monitoring programs, but failed to document or, if circumstances changed, revisit the risk-based rationale for the decision, again resulting in unidentified suspicious activity.

2017 FINRA Published Examination Findings (cont'd)

4. Resources for AML Monitoring

FINRA also identified deficiencies due to policies and procedures not being implemented as a result of firms not providing adequate resources to AML departments to carry out the responsibilities of the AML program. This result was more common when a firm experienced significant growth but did not grow the firm's AML program commensurately. The lack of resources can lead to deficient monitoring or inadequate investigations of potentially suspicious activity.

5. Independent Testing of AML Monitoring

FINRA also observed that some firms did not ensure the independent testing required under FINRA Rule 3310(c) included a review of how the firm's AML program was implemented. Other weaknesses included firms not ensuring the independence of the test, or not completing tests on an annual calendar year basis where the firm's business warranted that regular testing.

2018 FINRA Published Examination Findings

- FINRA's examination findings for 2018 identified three additional issues with broker-dealer AML programs:

1. Questionable Ownership Status of Foreign Legal Entity Accounts

FINRA has observed increased trading by foreign legal entity accounts in similar low-float and low-priced securities. In some instances, firms considered these accounts unrelated, but uncovered shared commonalities, which raised concerns about potential ownership or control by similar beneficial owners. Examples of these commonalities included trading directed from the same Internet Protocol locations, account funds sent from the same branches of a specific bank, accounts with the same authorized traders, and accounts established with the same mailing address.

2018 FINRA Published Examination Findings (cont'd)

2. No Documentation of Investigations of Potentially Suspicious Activity

Some firms that use exception reports did not document initial reviews and investigations into potentially suspicious activity identified by the reports. This was particularly troubling where those firms failed to establish and implement a formal investigation management process or document how they decided whether to file or not file Suspicious Activity Reports (SARs).

3. Irregular and Undocumented 314(a) Searches

FINRA has found that some firms failed to comply with Section 314(a) of the USA PATRIOT Act, and did not conduct reviews of FinCEN's Secure Information Sharing System (SISS) on a bi-weekly basis or did not document their reviews after the searches were complete. In other instances, firms also did not follow FinCEN's guidance to print a confirmation page from the SISS upon completing the review to evidence that they had performed the search and maintain records of positive search results.

Enforcement Actions Against Broker Dealers

- Central States Capital Markets, LLC – December 2018
  - SDNY announced first-ever criminal charges against a U.S. broker-dealer under the Bank Secrecy Act, and related DPA with a fine of $400,000
- UBS Financial Services – December 2018
  - $14.5 M penalty was shared with U.S. Treasury ($5 M), SEC ($5 M), and FINRA ($4.5 M)
- Morgan Stanley Smith Barney – December 2018
  - FINRA settlement and fine of $10 M

Broker-Dealer AML Takeaways

- Enforcement against broker-dealers for AML violations is on the upswing
- Broker-dealers should candidly evaluate whether their current programs, practices, and controls meet regulatory expectations
    - FINRA's examination findings are useful for understanding regulatory expectations, but each broker-dealer needs to consider the specific AML risks present in its business, and whether its AML program is sufficiently mitigating those risks

Financial Services for Cannabis Businesses

- General U.S. Legal Principles Governing Cannabis
- Department of Justice Policy
- FinCEN Policy
- Appropriations Amendments
- Legal Developments in 2018
- Outlook for 2019

LEXOLOGY® Webinars

CADWALADER

General U.S. Legal Principles Governing Cannabis

- **U.S. Federal Law**
  - The Controlled Substances Act ("CSA") (21 U.S.C. § 801 et seq.)
    - Cannabis is a Schedule I controlled substance; no legitimate medical use.
    - The CSA makes the manufacture, distribution and possession with intent to distribute marijuana a felony.
    - The CSA also criminalizes conspiracy to manufacture, distribute or possess with intent to distribute marijuana.
    - The CSA prohibits extraterritorial manufacture or distribution of controlled substances if the parties intend to import drugs into the United States.
- **U.S. State Law**
  - More than 30 states currently permit prescribing and dispensing marijuana for medical use.
  - At least eight states also permit adult use of recreational marijuana. In these states, a medical reason to grow, distribute, or dispense marijuana is not necessary.
  - In states that have either a medical or an adult-use scheme, there are generally detailed state regulations, including licensing requirements, that a business must follow to be compliant with state law.

Department of Justice (“DOJ”) Policy

- **2013 Cole Memo**
  - Instructed DOJ attorneys and law-enforcement officials to focus their marijuana-related CSA enforcement on eight enforcement priorities (e.g. funding gang activity)
  - Notes that, outside of these enforcement priorities, the federal government traditionally relies on state and local law-enforcement agencies to address marijuana activity through enforcement of their own narcotics laws
- **2014 Cole Memo**
  - DOJ will not prosecute marijuana-related financial crimes where federal enforcement priorities are not implicated

Financial Crimes Enforcement Network ("FinCEN") Policy

- **2014 FinCEN Guidance (FIN-2014-G001)**
  - Concurrent with the release of the 2014 Cole Memo.
    - Clarified BSA expectations for financial institutions seeking to provide services to Marijuana-Related Businesses ("MRBs").
    - Permissive structure: The stated goal in the guidance was to clarify "how financial institutions can provide services to MRBs consistent with their BSA obligations."
  - Made clear that state legalization of marijuana does not affect a financial institution's obligation to file a Suspicious Activity Report ("SAR") where the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution:
    - involves funds from illegal activity or is an attempt to disguise funds derived from illegal activity;
    - is designed to evade regulations promulgated under the BSA; or
    - lacks a business or apparent lawful purpose.

2014 FinCEN Guidance (cont'd)

- SARs must be filed for MRBs, which the guidance does not define.
- Three types of SARS defined (in ascending order of seriousness):
  - "*Marijuana Limited*" SAR Filing. A financial institution should file a "marijuana limited" SAR regarding an MRB that the financial institution "reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law . . . ."
    - SAR needs to contain only basic information about the subject or parties.
  - "*Marijuana Priority*" SAR Filing. Financial institutions should file a "marijuana priority" SAR regarding an MRB that the financial institution "reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law."
    - SAR "should include comprehensive detail" about the subject or parties and the enforcement priorities the financial institution believes are implicated.
  - "*Marijuana Termination*" SAR Filing. Financial institutions should file a "marijuana termination" SAR when the financial institution "deems it necessary to terminate a relationship" with an MRB "in order to maintain an effective" AML compliance program.
    - SAR should include "the basis for the termination."

2014 FinCEN Guidance (cont'd)

- Minimum Elements for Proper Due Diligence:
- In assessing the risk of accepting an MRB customer, financial institutions should conduct due diligence, including:
  - Verifying with the appropriate state authorities whether the business is duly licensed and registered;
  - Reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate as an MRB;
  - Requesting from state licensing and enforcement authorities available information about the business and related parties;
  - Developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served;
  - Ongoing monitoring of publicly available sources for adverse information about the business and related parties,;
  - Ongoing monitoring for suspicious activity, including for any of the red flags described in the guidance; and
  - Refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk.

FinCEN Marijuana Banking Update (Dec. 2018)

FinCEN
Financial Crimes Enforcement Network / Intelligence Division

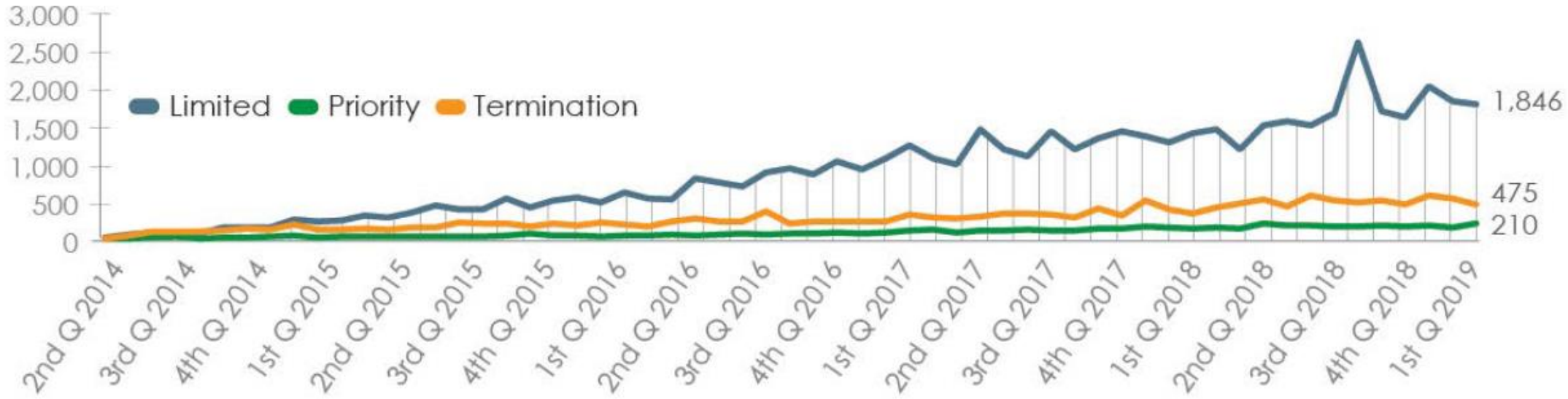
LEXOLOGY® Webinars

CADWALADER

FinCEN Marijuana Banking Update (Dec. 2018)

FinCEN
Financial Crimes Enforcement Network / Intelligence Division

Monthly Totals for Marijuana Guidance SARs by Key Phrase



LEXOLOGY® Webinars

CADWALADER

Appropriations Amendments

- First passed in 2014, Rohrabacher-Blumenauer (then known as Rohrabacher-Farr) is an amendment to the annual appropriations bill that prohibits the DOJ from using federal funds to interfere with state legal medical marijuana programs.
  - Only applies to medical marijuana cases.
  - The appropriations prohibition has been upheld in court as prohibiting federal prosecutions against medical marijuana growers.
  - As a part of the annual appropriations budget, this amendment needs to be renewed each time a new budget passes.
- A measure to apply appropriations prohibitions like the Rohrbacher amendment to FinCEN was voted down in the house.

Cannabis-Related Legal Developments in 2018

- January 2018
  - The 2013 and 2014 Cole Memos were rescinded.
    - Federal prosecutors are no longer required to decline prosecution of state legal MRBs. Instead they are to consider their resources and balance equities appropriately.
  - FinCEN guidance was not rescinded.
    - But given its reliance on the Cole Memo, it is of somewhat less comfort than it was previously.
- June 2018
  - Senators Warren and Gardner sponsored a bill (STATES Act) which provides that the CSA does not apply to any person acting in compliance with the cannabis legalization laws of their states. Senator McConnell said he would allow this bill to come to the floor for a vote, and President Trump even indicated he might support it.
    - If enacted as law, the bill would likely change the analysis on the AML risks inherent in banking MRBs outside the United States. It will largely depend on the wording of the bill.

Banking Developments

- Although some banks serve MRBs, the situation remains difficult:
  - Costs: Many banks charge high fees for MRBs
  - Instability: Banks that publicized their services to MRBs have changed course (M Bank, First Security Bank of Nevada)
  - No new banks for MRBs: The Federal Reserve denied a master account to The Fourth Corner Credit Union (TFCCU), a new CU which explicitly included MRBs in its field of membership
  - A Federal Court held that TFCCU had no right to a master account
- Fintech startups have attempted to fill the banking void by enabling cashless transactions, but have shortcomings:
  - Do not eliminate BSA obligations of banks that ultimately receive funds
  - Lack sufficient network effects to be attractive to MRBs

Outlook for 2019

- SAFE Banking Act
  - Designed to give financial institutions comfort sufficient to provide services to cannabis-related businesses
  - Defines “cannabis-related legitimate business” and “service provider”
  - If enacted as law:
    - Would make clear that a transaction does not involve proceeds of an unlawful activity under 18 U.S.C. § 1956 *solely* because the transaction involves a state-authorized cannabis-related legitimate business or service provider;
    - Would protect a financial institution’s officers, directors, and employees from liability under any Federal law or regulation *solely* for providing financial services to a state-authorized cannabis-related legitimate business or service provider; and
    - Would require FinCEN to issue (and financial institutions to follow) special SAR-filing guidance.
  - First-ever House hearing on marijuana-related banking was held in February 2019
- Legalization of Cannabis in Canada
  - Has generated a number of questions about whether and how a U.S. financial institution can provide financial services, including IPO underwriting and share custody services, to Canadian cannabis businesses

AML for Cryptocurrencies & Digital Assets

- Blockchain technology
- Cryptocurrencies and digital assets
- Anonymity
- AML for “Money Services Businesses”
- Financial Institutions serving cryptocurrency or digital asset businesses
- Financial Institutions that are cryptocurrency or digital asset businesses
- Latest developments

LEXOLOGY® Webinars

CADWALADER

Blockchain Technology

- Blockchain & Distributed Ledger Technology
  - Blockchain is a shared, digitized ledger designed to be unchangeable once a transaction has been recorded and verified
  - The ledger is available to all parties to the transaction, and many third parties, making it difficult to amend every copy of the ledger globally to fake a transaction
- Blockchain technology offers many advantages and some disadvantages
  - Peer-to-peer global transactions
  - Permits traceability (immutable record on all network devices, with time stamps)
- For AML purposes, there are two key considerations:
  - Blockchain's ability to move value; and
  - Blockchain's pseudonymous nature

Cryptocurrencies & Digital Assets

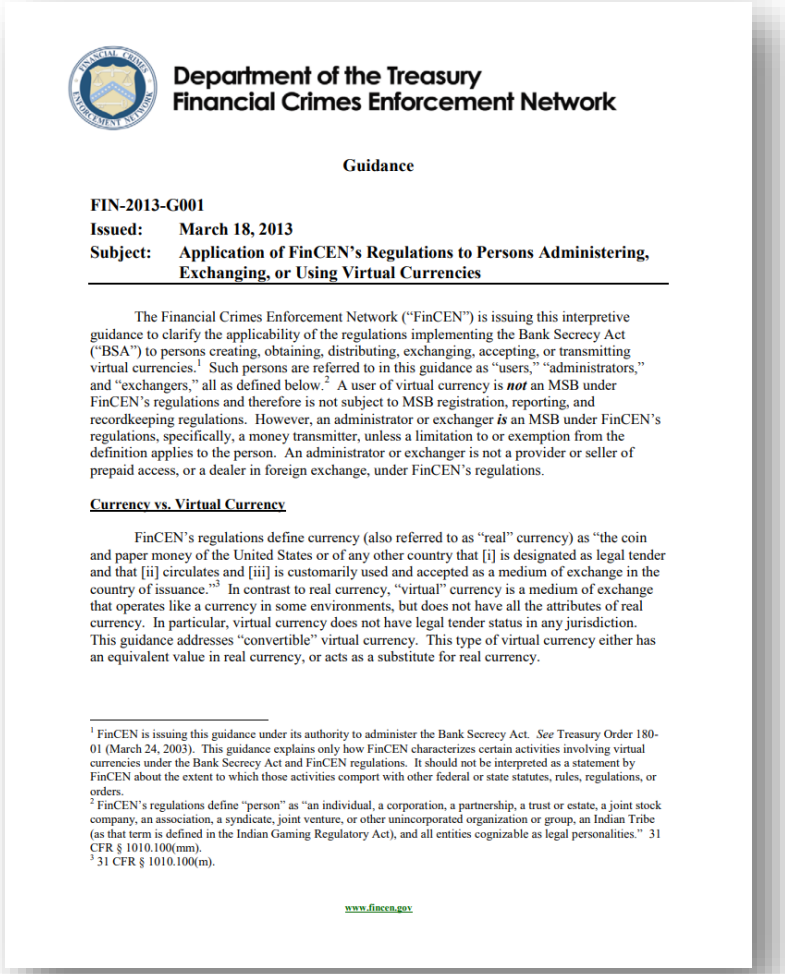
- There is no single set of definitions used by regulators, market participants or others to describe assets represented on blockchain.
- For our purposes, there are three categories to consider:
  - Cryptocurrency / Virtual Currency
    - E.g. Bitcoin or Ethereum, which regulators generally treat as funds
  - Initial Coin Offerings (“ICOs”)
    - Regulators generally treat as a security
  - Utility Tokens
    - Grant a right to use an application or service. Regulators are divided.
- Despite the wishes of many crypo-enthusiasts, most U.S. regulators (CFTC, FinCEN, IRS, SEC, NY DFS) take the view that crypto assets are likely either a security or a virtual currency

Anonymity

- CDD on customers is controversial with some crypto-enthusiasts who value anonymity
- U.S. regulations do not prevent “users” from transacting directly and anonymously with one another
    - Just as I could anonymously give $5 cash to a street vendor selling flowers, a “user” can anonymously send cryptocurrency directly from one personal digital currency address to another personal digital currency address
    - But when a person is “in the business” of providing payments, custody, and exchange services the BSA treats it as a financial institution offering the same services for funds or securities
- Anonymity may be popular, but under the BSA a financial institution should not permit it
- For BSA purposes, who is a financial institution?

AML for “Money Services Businesses” (MSBs)

- 2013 FinCEN Virtual Currency Guidance (FIN-2013-G001)
  - Definitions:
    - “Users” obtain virtual currency to purchase goods or services
    - “Exchangers” are persons engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency
    - “Administrators” are persons engaged as a business in issuing (putting into circulation) a virtual currency, and who have the authority to redeem (to withdraw from circulation) such virtual currency



Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2013-G001
Issued: **March 18, 2013**
Subject: **Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies**

The Financial Crimes Enforcement Network (“FinCEN”) is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act (“BSA”) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.[1] Such persons are referred to in this guidance as “users,” “administrators,” and “exchangers,” all as defined below.[2] A user of virtual currency is ***not*** an MSB under FinCEN’s regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger ***is*** an MSB under FinCEN’s regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN’s regulations.

Currency vs. Virtual Currency

FinCEN’s regulations define currency (also referred to as “real” currency) as “the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance.”[3] In contrast to real currency, “virtual” currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses “convertible” virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.

[1] FinCEN is issuing this guidance under its authority to administer the Bank Secrecy Act. *See* Treasury Order 180-01 (March 24, 2003). This guidance explains only how FinCEN characterizes certain activities involving virtual currencies under the Bank Secrecy Act and FinCEN regulations. It should not be interpreted as a statement by FinCEN about the extent to which those activities comport with other federal or state statutes, rules, regulations, or orders.
[2] FinCEN’s regulations define “person” as “an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.” 31 CFR § 1010.100(mm).
[3] 31 CFR § 1010.100(m).

www.fincen.gov

2013 FinCEN Virtual Currency Guidance

- A person has AML obligations under the Bank Secrecy Act if it is a "money services business" ("MSB")
- "Users" are generally not MSBs and thus not subject to the BSA
- "Money transmitters" are MSBs and thus subject to the BSA's AML requirements
  - Both "exchangers" and "administrators" of virtual currency are "money transmitters" if they:
    - Accept and transmit a convertible virtual currency; or
    - Buy or sell convertible virtual currency for any reason.

2013 FinCEN Virtual Currency Guidance (cont'd)

- Persons that are MSBs must do the following:
  - Register with FinCEN as an MSB
  - Establish a written risk-based AML program
  - Appoint a compliance officer
  - Train employees
  - Maintain records of funds transmitted
  - File currency transaction reports ("CTRs") and suspicious activity reports ("SARs")
    - SAR threshold for MSBs is $2,000 – lower than for other financial institutions
  - Comply with the Transfer Rule (for transfers over $3,000) and Travel Rule
  - Conduct independent testing of the AML program and controls
- 2014 guidance addressed the application of FinCEN's regulations to virtual currency mining operations, virtual currency software development, and certain investment activity (*See* FIN-2014-R001 & FIN-2014-R002)

Financial Institutions that Serve Cryptocurrency and Digital Asset Businesses

- CDD on customers should include:
  - Customer identification
    - What is the business? Is the customer meeting appropriate regulatory requirements?
      - Is it a registered MSB? If so, review its AML program.
      - Is it an unregistered business that should be registered as an MSB? If so, ask why and consider whether it is appropriate to accept or keep the customer.
      - Is it an issuer of an unregistered security?
      - Is it an unregistered exchange or broker-dealer in securities?
    - Who is behind the business?
    - Is there material negative information in the public domain about the business or its promoters? ICO fraud, hacks, and sales of unregistered securities are common.

Financial Institutions that Are Cryptocurrency and Digital Asset Businesses

- First things first: Be ready to explain your business, MSB status, and any AML program to your bank
- CDD on customers should answer the following questions:
    - Is the customer a "user?" If the customer is a business, what is the business? A falafel shop? A crypto exchange? Is the customer meeting appropriate regulatory requirements? (Same inquiries as previous slide)
    - Which digital currency address(es) does the customer control?
- Monitoring and controls
    - What is the expected transactional profile for the customer? Are transaction limits appropriate?
    - If enabling payments to third parties, screen those third parties' digital addresses and names (if known) against known lists of high-risk persons (e.g. OFAC's SDN list, commercially available lists)
        - This includes monitoring digital addresses for the proceeds of hacks or fraud, and the use of "mixers" or "tumblers" designed to obfuscate the identity of persons associated with digital addresses

Latest Developments

- **February 2018:** FinCEN letter to Senator Wyden
    - Emphasized that IRS examines MSBs for AML compliance, whereas SEC and CFTC have jurisdiction over AML matters related to securities and derivatives. Also said issuers of ICOs may by MSBs
        - (Note: most money transmitters are also bound by state registration and inspection requirements)
- **September 2018:** SEC brought first enforcement action against a person (TokenLot LLC**)** who allegedly acted as an unregistered broker-dealer in connection with the sale of ICO tokens
- **October 2018:** FATF Recommendations updated to define "virtual assets" and to require countries to subject "virtual asset service providers" to AML/CFT regulation
    - FATF's flexible requirements are unlikely to be a catalyst for regulatory harmonization around the globe
- **November 2018:** OFAC doxes the blockchain
    - OFAC stunned some crypto enthusiasts by publicly identifying the digital currency addresses of two individuals named to the SDN list
    - OFAC also stunned some crypto businesses by making clear that they are expected to comply with OFAC requirements by screening the digital currency addresses they do business with

Latest Developments (cont'd)

- **February 2019**: SEC enforcement action against Gladius Network ICO
  - Until recently, SEC enforcement primarily focused on fraud – ICOs making untrue statements to solicit funds
  - Then Gladius Network LLC raised $12.7 million from 1,700 investors in 2017, when it publicly offered and sold its own proprietary digital coins in exchange for an established digital currency
  - SEC charged Gladius with offering unregistered securities; Gladius settled with SEC and registered the securities
- **March 2019**: American Bar Association published "Digital and Digitized Assets: Federal and State Jurisdictional Issues"
  - 353-page tome
  - Describes how existing regulatory regimes for securities regulation and money transmission apply to digital assets
  - Includes a 50-state survey and overview of regulatory developments in Europe and Asia
- **Ongoing**:
  - Regulatory positioning for blockchain dominance: Bermuda (ICO legislation), Bahamas (digital currency pilot), Gibraltar ("DLT Regulatory Framework"), Malta ("the Blockchain Island")

Looking Ahead in AML

- Growing synergies between AML and sanctions enforcement and compliance programs
- AML regulators' encouragement of "innovative approaches" (i.e. artificial intelligence)
- Expansion of FinCEN's real estate geographic targeting orders
- European Commission blacklisting U.S. territories as AML-deficient
- Draft legislation to amend key aspects of the Bank Secrecy Act

Growing Synergies Between AML & Sanctions Programs

- **December 2018**: Treasury published a speech in which Under Secretary Sigal Mandelker described "hallmarks of an effective sanctions program." The "hallmarks" are highly similar to the "pillars" of an effective AML program:
  - Ensuring senior management commitment to compliance;
  - Conducting frequent risk assessments to identify and mitigate sanctions-specific risks within an institution and its products, services, and customers;
  - Developing and deploying internal controls, including policies and procedures, in order to identify, interdict, escalate, report, and maintain records pertaining to activity prohibited by OFAC's regulations;
  - Engaging in testing and auditing, both on specific elements of a sanctions compliance program and across the organization, to identify and correct weaknesses and deficiencies; and
  - Ensuring all relevant personnel, particularly those in high-risk areas or business units, are provided tailored training on OFAC obligations and authorities in general and the compliance program in particular.
- **February 2019**: OFAC Venezuela FAQ 650 states, "OFAC expects U.S. persons to conduct due diligence on their own direct customers"
- Recent settlements point to OFAC's view that these "hallmarks" are an industry best practice.
- **Takeaway**: Sanctions programs may begin to look more like AML programs.

Artificial Intelligence

- December 3, 2018: Joint Statement from FinCEN, the Federal Reserve, FDIC, NCUA and OCC (the "Agencies") on "Innovative Efforts to Combat Money Laundering and Terrorist Financing"
  - Stated goal is "to encourage banks to consider, evaluate, and [. . .] responsibly implement innovative approaches to meet [. . .] BSA/AML compliance obligations
  - The Agencies "will not penalize or criticize" a bank that does not use innovative approaches, if its BSA/AML program is effective and commensurate with the bank's risk profile
  - Pilot programs "should not" subject banks to regulatory action if the pilot is unsuccessful or the pilot exposes compliance gaps – the Agencies will assess existing processes independent of the results of any pilot program
  - Bank management should "prudently evaluate whether, and at what point, innovative approaches may be considered sufficiently developed to replace or augment existing BSA/AML processes"
- The Joint Statement is merely guidance, and is not binding on the Agencies
- As a result, banks can take only limited comfort

Expansion of the Real Estate GTOs

- FinCEN's real estate geographic targeting orders (GTOs) have, in various forms, been in place since 2016.
- They require title insurance agencies to collect information about the individual beneficial owner(s) of specified residential real estate, when a legal entity purchases the property without a U.S. bank loan.
- The orders initially applied only to purchases of $3 million in Manhattan and $1 million in Miami, but other cities have been added.
- In November 2018, FinCEN dropped the threshold to $300,000, and included transactions conducting in virtual currency, greatly expanding the GTO's reach.
- The GTO regime is still temporary, but legislation could make it permanent.
- H.R. 389 would require FinCEN to expand the current GTO to cover commercial real estate transactions as well.

European Commission Blacklisting U.S. Territories

- **February 13, 2019**: the European Commission published a list of jurisdictions it identified as having strategic AML/CFT deficiencies.
- The list included 12 jurisdictions already on the FATF list of jurisdictions with strategic deficiencies, and added 11 additional jurisdictions, including the U.S. territories of American Samoa, Guam, Puerto Rico and the U.S. Virgin Islands.
- The U.S. Treasury rejected the list, stating that it has "significant concerns about the substance of the list and the flawed process by which it was developed."
- Treasury stated that it does not expect U.S. financial institutions to take the European Commission's list into account in their AML/CFT policies and procedures.
- **March 7, 2019**: EU Member States unanimously reject the EC list as "not established in a transparent and resilient process."
- **Summer 2019**: The EC is expected to publish a new list.

Draft Amendments to the BSA

- Various drafts of legislation that would amend the BSA have been introduced in the past 18 months
- Earlier drafts included:
  - Changes to the SAR and CTR thresholds (raising as high as $30,000 or pegging to inflation)
  - Requirements that persons registering companies file beneficial ownership information with FinCEN
- The latest draft includes:
  - Broader sharing of suspicious activity reports within a financial group
  - Additional damages for repeat Bank Secrecy Act violators
  - Prohibition on tax deductions for attorney fees related to Bank Secrecy Act settlements and court costs
  - Application of Bank Secrecy Act to dealers in art or antiquities
  - Encouragement for the use of technology in BSA compliance
- Will this be the big year that amendments are passed?

Contact

Jodi Avergun
Jodi.Avergun@cwt.com

Todd Blanche
Todd.Blanche@cwt.com

Joseph V Moreno
Joseph.Moreno@cwt.com

Christian Larson
Christian.Larson@cwt.com

LEXOLOGY® Webinars

CADWALADER