Keeping Up with Anti-Money Laundering Rules

July 19, 2022

By: Andrew Bigart and Preston Neel

OLA
Online Lenders Alliance

Today's Speakers

Andrew E. Bigart
Partner
Venable LLP

aebigart@Venable.com
202.344.4323

Preston H. Neel
Partner
Bradley Arant Boult Cummings LLP

pneel@bradley.com
205.521.8491

Online Lenders Alliance

Agenda

- Review of the Legal Framework for BSA/AML
- Review of Developments in Beneficial Ownership / Corporate Transparency Act
- Hot Topics
  - Cryptocurrency
  - Use of AI and ML in AML Monitoring
  - FinCEN RFI on Modernization of AML/CFT Regime
- Enforcement Review
- Best Practices / Areas for Risk Monitoring

Review of the Legal Framework for BSA/AML

Overview: Legal Framework of the Bank Secrecy Act

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act, commonly known as the "Bank Secrecy Act" (BSA). The BSA is often referred to as an "anti-money laundering" (AML) law or jointly as "BSA/AML." The BSA granted the Secretary of the Treasury authority to impose regulations on insured banks.

The Bank Secrecy Act comprises 12 separate legislative acts, including the USA PATRIOT Act and the Anti-Money Laundering Act of 2020.

Other major U.S. AML laws include:

- Money Laundering Control Act (1986)
- Anti-Drug Abuse Act of 1988
- Annunzio-Wylie Anti-Money Laundering Act (1992)
- Money Laundering Suppression Act (1994)
- Money Laundering and Financial Crimes Strategy Act (1998)
- Intelligence Reform and Terrorism Prevention Act of 2004

Overview: Legal Framework of the Bank Secrecy Act

- **AML**

When the BSA was initially enacted, it established requirements for recordkeeping and reporting by private individuals, banks, and other financial institutions. It was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States. It required banks and other financial institutions to:

- Report cash transactions over $10,000 using the Currency Transaction Report (CTR)
- Properly identify persons conducting transactions
- Maintain a paper trail by keeping appropriate records of financial transactions.

The Money Laundering Control Act of 1986 made money laundering a federal crime.

Jurisdictional Oversight

Certain government agencies play a critical role in implementing BSA regulations, developing examination guidance, ensuring compliance with the BSA, and enforcing the BSA. These agencies include the following:

- U.S. Treasury
- FinCEN
- Federal Financial Institutions Examination Council, i.e., federal banking agencies
    - Board of Governors of the Federal Reserve System (Federal Reserve);
    - Federal Deposit Insurance Corporation (FDIC);
    - National Credit Union Administration (NCUA); and
    - Office of the Comptroller of the Currency (OCC)

Jurisdictional Oversight

- **FinCEN**

In 1990, the Financial Crimes Enforcement Network (FinCEN) was established as a bureau of the U.S. Treasury Department. The initial goals were to analyze data and track financial criminals.

In 1992, the Annunzio-Wylie Anti-Money Laundering Act required financial institutions to report suspicious activity. FinCEN served a key role in 2005 when the first Federal Financial Institutions Examination Council (FFIEC) released its joint examination manual.

Today, FinCEN works closely with federal and state law enforcement authorities in its capacity as BSA administrator. It regularly releases updates to existing regulations and solicits feedback from various industries.

The Four Pillars of BSA

"The Four Pillars…"

- Designation of a BSA Compliance Officer
- Development of Internal Policies, Procedures, and Controls
- Ongoing, Relevant Training of Employees
- Independent Testing and Review

AND the unofficial fifth pillar: Customer Identification Program (CIP)

The FFIEC Manual encompassed the first clear breakdown of the critical pillars of a BSA/AML Program.

These pillars would ultimately form the core examination review by regulators.

The Four Pillars of BSA: Bank Secrecy Act Officer

- Annually, the Board of Directors must approve a BSA Officer.
    - The BSA Officer must be provided the tools and training to effectively manage the BSA program.
    - The BSA Officer must also possess the authority sufficient to manage the BSA/AML Program.

The Four Pillars of BSA: Written Program and Internal Controls

Internal controls are comprised of policies, procedures, and controls. The FFIEC Manual breaks down the level of sophistication of internal controls, to depending on the size and scale of the institution;. However, internal controls should conform to the following guidelines:

- The written program should be revisited and revised annually based on the results of the financial institution's BSA/AML/OFAC Risk Assessment.
- The written program must be approved by the Board annually.
- The written program should be commensurate with the size and complexity of the Bank.
- Internal controls prescribed in policies and procedures should be based on the risk assessment and the size and complexity of the entity.

The Four Pillars of BSA:Training

Without proper training, staff might leave an institution too exposed to significant money laundering risk. There are several components of a training program that the FFIEC Manual dictates:

- Personnel must receive annual BSA/AML/OFAC training.
- The Board of Directors must also receive annual training.
- The materials used and attendance records must be kept on file.
- New employees should receive training prior to on-boarding during an orientation.
- Training must be tailored to the individual's responsibilities tied to BSA/AML/OFAC compliance.

The Four Pillars of BSA: Independent Testing

Independent testing provides verification of whether your compliance program is operating as effectively as possible and is compliant with the law.

- Financial institutions are required to conduct annual independent testing of the BSA/AML/OFAC program.
- Testing may be done internally if the personnel are truly independent from the processes and implementation of the BSA program.
- It is permissible to engage with an outside 3rd party for testing.
- Testing should be comprehensive.
- Results of the testing should be communicated to the Board / Executive Management in a timely manner.
- The implementation of recommendations and correction of findings should be tracked with periodic progress reports to the Board. *This is Critical.

Customer Identification Program (CIP)

- Financial institutions are required to have a written Customer Identification Program.
- CIP is intended to allow the institution to reasonably believe that it knows the true identity of each customer.
- The program must include account opening procedures specifying the required identification for opening an account.
- The program must also include procedures for verifying the identity of each customer.
    - At a minimum you must obtain the following identifying information from each customer before opening an account:
        - Legal Name (Individual or Business)
        - Date of Birth (individuals)
        - Physical Address
        - Identification Number (SSN, TIN, Passport Number, Foreign Alien ID Number)
        - Documentation (Articles of Incorporation, Doing Business As (DBA) Paperwork, etc.)

Customer Identification Program (CIP)

- Customer identities should be verified using risk-based procedures.
- Appropriate procedures for various circumstances should be addressed in the program.
  - Document Verification: Driver's License
  - Nondocumentary Methods: Third Party Consumer Reporting Agencies
- The program should address:
  - Circumstances when an account should not be opened
  - Circumstances that require more due diligence in confirming the consumer's identity
  - When an account should be closed
  - When a SAR should be filed based on false identification or other suspicious activity

General Reporting Requirements

- Suspicious Activity Reports (SARs)
- Currency Transaction Reporting (CTR)
- Form 8300

Suspicious Activity Reporting

Certain financial institutions and other businesses subject to the US AML program requirements must file Suspicious Activity Reports (SARs). SARs are generally required when a financial institution "knows, suspects, or has reason to suspect" that a transaction conducted or attempted by, at, or through the financial institution involving at least $5,000 ($2,000 for MSBs and $25,000 or more for banks when the suspect is unknown):

- Involves money laundering;
- Is designed to evade any BSA regulation or requirement;
- Has no business or apparently lawful purpose, or is not the type of transaction in which that customer would be expected to engage; or
- Involves the use of the financial institution to facilitate criminal activity.

Review of Developments in Beneficial Ownership / Corporate Transparency Act

Anti-Money Laundering Act of 2020

- Effective Jan. 1, 2020, Congress enacted the Anti-Money Laundering Act of 2020 (the Act), the most significant AML legislation in decades.
  - Encourages a risk-based approach to AML compliance
  - Expands BSA coverage to new categories of financial institutions
    - Persons engaged in the trade of antiquities
    - Virtual currency businesses that qualify as money transmitters
  - Expands whistleblower rewards and protections
  - BSA has provisions authorizing whistleblower payments, but has had minimal impact in past. The Act expands the program and amount of payments to encourage more reporting.

Anti-Money Laundering Act of 2020

- Corporate Transparency Act (CTA) (part of the AML Act of 2020)
  - Direction to FinCEN to establish a beneficial ownership registry
  - U.S. regulators have been pushing to increase beneficial ownership reviews for years; the Act requires FinCEN to implement a registry of beneficial owners for certain "reporting companies" to facilitate such reviews and monitoring.
  - Codifies FinCEN's beneficial ownership rule.
- New BSA violations and enhanced penalties for repeat and egregious violators
  - Act criminalizes misrepresentation of material facts to an FI concerning the ownership of assets involved in a monetary transaction if the owner of the asset is a senior foreign political figure.
  - Act makes it a crime to knowingly misrepresent a material fact to an FI about the source of funds in a monetary transaction that involves an entity identified by Treasury as a primary money laundering concern.
  - Act includes increased civil penalties for repeat and egregious BSA violators.

Corporate Transparency Act (CTA)

- In December 2021, FinCEN issued the first in an expected series of notices of proposed rulemaking (NPRMs) to implement the beneficial ownership information (BOI) reporting provisions of the Corporate Transparency Act (CTA).
- Goal of the NPRM is to protect the U.S. financial system from illicit use and impede malign actors from abusing legal entities, like shell companies, to conceal proceeds of corrupt and criminal acts.
- Focus is to stop bad actors from using legal entities to hide illicit funds behind anonymous shell companies or other opaque corporate structures.
  - First NPRM focused on who must file a BOI report, what information must be reported, and when a report is due.
  - Future NPRMs to address (1) who may access BOI, for what purposes, and what safeguards will be required to ensure that the information is secured and protected; and (2) revise FinCEN's customer due diligence rule following the promulgation of the BOI reporting final rule.
- FinCEN is developing the infrastructure to administer these requirements, such as the BOI technology system.

Corporate Transparency Act (CTA)

- Reporting Companies
  - A domestic reporting company would include a C-corp, LLC, or any other entity created by the filing of a document with a state (e.g., partnerships, certain trusts).
  - A foreign reporting company would include a C-corp, LLC, or other entity formed under foreign law.
  - 23 types of entities exempt from the definition of "reporting company," such as regulated FIs, companies traded on exchanges, and even companies with more than 20 employees (under certain circumstances).
- Beneficial Owners
  - NPRM defines a beneficial owner as any individual who (1) exercises substantial control over a reporting company, or (2) owns or controls at least 25 percent of the ownership interests of a reporting company.
- Beneficial Ownership Information Reports
  - Need to report four pieces of information about each beneficial owner and company applicants: name, birthdate, address, and a unique identifying number from an acceptable ID document (and the image of such document).
- Timing
  - Reporting companies created before the final rule would have a year to file their initial reports; reporting companies created or registered after the final rule would have 14 days after their formation to file.
  - Reporting companies would have 30 days to file updates to their previously filed reports, and 14 days to correct inaccurate reports after they discover or should have discovered the reported information is inaccurate.

Corporate Transparency Act (CTA)

- Implications for Reporting Companies
  - Companies should review the CTA/NPRM to determine whether they will be considered a reporting company.
  - Willful failure to report, or the submission of a report containing false or fraudulent beneficial ownership information, is subject to penalties.
- Implications for Financial Institutions
  - The BSA requires certain financial institutions, including banks, to develop and maintain an effective AML program, including customer due diligence. The requirement to identify and verify the identity of beneficial owners of legal entity customers was imposed by FinCEN in 2016. The CTA will provide financial institutions with a means to verify the information on reporting companies, thereby increasing the effectiveness of the AML program.

Hot Topics

Hot Topics – Cryptocurrency

- FinCEN and several state regulators have published guidance stating that the movement of monetary value through virtual currencies may trigger money transmitter obligations.
- FinCEN and state regulators generally define regulated virtual currency as one that (1) has an equivalent value in fiat currency or (2) acts as a substitute for fiat currency.
  - I.e., a convertible virtual currency (CVC)
- Other risks
  - Securities (SEC)
  - Commodities/derivatives (CFTC)
  - OFAC
  - Unclaimed property
  - Advertising and consumer protection risks

Hot Topics – AI and ML in AML

- Financial institutions are exploring how best to leverage developments in AI and ML for credit decisioning and AML efforts.
  - AI is a term used to address various technologies and systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.
  - Machine learning (ML) refers to algorithms that improve their performance through the sharing or analysis of pattern information.

Hot Topics – AI and ML in AML

- When it comes to AML, current systems tend to be rule-based and in many cases manual, requiring review of various data points against established requirements and rules (both with respect to identifying customers and for monitoring suspicious activity).
  - AI and ML can be used to improve and monitor the determinations made by employees engaged in performing various compliance functions, including customer onboarding and transaction monitoring and investigations.
  - Increasingly, financial institutions are using AI to confirm customer identity by collecting and comparing traditional, publicly available data used for verification (name or address) with data from non-traditional sources, such as an access device's IP address or biometric data.

Hot Topics – AI and ML in AML

- The use of AI/ML by a financial institution for customer identification, verification, and related purposes appears consistent with this legal framework, provided that the financial institution implements these technologies consistent with regulatory expectations.
  - In 2018, FinCEN and the banking regulators issued a joint statement recognizing the use of AI by FIs in their AML programs, and noted AI's potential to improve compliance and efficiency.
  - As explained by a former director of FinCEN in 2019, U.S. federal regulators are "committed to working with industry on ways in which technological advances with respect to identity can fit within our current regulatory framework or may lead to changes in our regulations."
  - In 2021, the federal banking regulators issued a Request for Information (RFI) seeking industry input on the use of AI and ML for operational and regulatory compliance purposes. Numerous comments were submitted by trade associations, companies, and consumer advocates.
  - FinCEN established an Innovation Hours Program that serves as a forum for policymakers and industry to discuss innovative products and services, such as AI and digital identity.

Hot Topics – Modernization of AML Regime

- FinCEN continues to explore ways to streamline, modernize, and update BSA regulations and guidance.
  - FinCEN seeks to promote a risk-based approach to protecting the financial system while also providing for the reporting of information with a high degree of usefulness to government authorities.
- FinCEN issued a request for information in December 2021
  - Focus on reviewing the records and reports that FIs are required to maintain / submit
  - Review FinCEN regulations to identify guidance that is outdated or in need of updating
- Industry submitted comments such as:
  - Streamline currency transaction reporting.
  - Increases to reporting thresholds.
  - Encourage risk-based approach to account monitoring.

Enforcement Review

Online Lenders Alliance

Enforcement Review

Capital One

- On January 15, 2021, FinCEN announced that it assessed a civil monetary penalty of $390 million against Capital One for violations of the BSA related to Capital One's Check Cashing Group (the "CCG").
- CCG was previously a business unit under Capital One's commercial bank until 2014, through which Capital One provided banking services including processing checks and providing customers with armored car cash shipments.
- In issuing its decision, FinCEN determined that, between 2008 and 2014, Capital One's CCG failed to report millions of dollars in suspicious transactions. Specifically, FinCEN found that Capital One:
  - failed to maintain an AML program to guard against money laundering per 31 U.S.C. § 5318(h);
  - failed to file suspicious activity reports (SARs) on suspicious transactions in violation of 31 U.S.C. § 5313; and
  - failed to file currency transaction reports (CTRs) for the CCG in violation of 31 U.S.C. § 5313.

Enforcement Review

BitMEX

- On August 10, 2021, FinCEN announced that it assessed a civil monetary penalty of $100 million against BitMEX, a convertible virtual currency derivatives exchange that offers futures, options, and swaps in cryptocurrencies.
- FinCEN found that between 2014 and 2020, BitMEX violated the BSA by failing to implement an adequate anti-money laundering program, verify customers' identities, and file SARs in at least 588 transactions.
- As FinCEN explained, "BitMEX conducted at least $209 million worth of transactions with known darknet markets or unregistered money services businesses providing mixing services," and some transactions involved "high-risk jurisdictions and alleged fraud schemes." BitMEX also failed to implement adequate controls to ensure it did not conduct business with persons located in the United States and in some cases, even altered customers' location information.

Best Practices / Areas for Risk Monitoring

Best Practices – AML and CFT National Priorities

- June 30, 2021: FinCEN, OFAC, banking regulators, and others developed the first government-wide priorities for AML/CFT.
  - Corruption; cybercrime, including relevant cybersecurity and virtual currency considerations; foreign and domestic terrorist financing; fraud; transnational criminal organization activity; drug trafficking organization activity; human trafficking and human smuggling; and proliferation financing.
  - Fraud—such as bank, consumer, health care, securities and investment, and tax fraud—is believed to generate the largest share of illicit proceeds in the United States.
- FinCEN will issue regulations at a later date that will specify how financial institutions should incorporate these priorities into their risk-based AML programs

Best Practices – Recent FinCEN Advisories

- June 15, 2022: Advisory on Elder Financial Exploitation
  - Elder financial exploitation (EFE) involves the illegal or improper use of an older adult's funds, property, or assets, and is often perpetrated through either theft or scams.
  - Older adults are targets for financial exploitation because of their income and savings, the possibility of declining cognitive or physical abilities, isolation from family and friends, lack of familiarity or comfort with technology, and reliance on others.
  - Common scams
    - Government imposter scams
    - Romance scams
    - Emergency/person-in-need scams
    - Lottery and sweepstakes scams
    - Tech and customer support scams
  - Advisory provides examples of various types of red flags of potential scams

Best Practices – Recent FinCEN Advisories

- March 7, 2022: Red Flags on Potential Russian Sanctions Evasion Attempts
  - Advises to be vigilant against potential efforts to evade the expansive sanctions and other U.S.-imposed restrictions implemented in connection with the Russian Federation's further invasion of Ukraine.
  - Examples of red flags include:
    - Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.
    - Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale.
    - Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate
- March 16, 2022: Alert on Real Estate, Luxury Goods, and Other High Value Assets Involving Russian Elites, Oligarchs, and Their Family Members
  - Warns that real estate, luxury goods, and other high-value assets can be used as a store of value, a medium of exchange, or an investment that sanctioned Russian elites and their proxies may use such assets to evade expansive U.S. and other sanctions

Best Practices – Recent FinCEN Advisories

- February 2, 2021: Advisory on COVID-19 Health Insurance and Health Care-Related Fraud
  - Alert financial institutions to health insurance and health care frauds related to the COVID-19 pandemic.
  - Frauds target Medicare, Medicaid/Children's Health Insurance Program (CHIP), and TRICARE, as well as health care programs provided through the Departments of Labor and Veterans Affairs (collectively, "health care benefit programs") and private health insurance companies.
  - Examples of scams include:
    - Unnecessary services
    - Billing schemes
    - Kickbacks
    - Health care technology schemes
    - Telefraud and telehealth schemes
    - Identity theft

Best Practices – Red Flags

- Account Opening
  - Concern about compliance with government reporting requirements and lender policies, particularly with respect to verifying identity, type of business, and assets
  - Customer uses unusual or suspicious identification documents that cannot be readily verified
  - Customers attempting to conceal their identity in online loan applications.
  - Borrower refuses, upon request, to identify or fails to indicate any legitimate source of his or her funds or assets
  - Customer provides an individual taxpayer identification number after having previously used a Social Security number
  - Borrower exhibits a lack of concern about risks, fees, or other transaction costs

Best Practices – Red Flags

- Account Opening (cont).
  - Borrower provides incomplete or false information, or information that is contradicted by or is inconsistent with information obtained from reputable third parties, such as consumer reporting agencies, during the application process or any routine request for updated information
  - Borrower has difficulty describing the nature of his or her business or lacks general knowledge about the industry
  - Two or more unrelated customers use the same or similar addresses and/or telephone numbers
  - Customer has multiple accounts under a single name or multiple names with a large number of inter-account or third-party transfers, without apparent reason
  - Customer has multiple accounts, or maintains accounts in the names of family members or related corporate entities for no apparent business or legitimate reason
- Transactions
  - Borrower is reluctant to provide information necessary for lender to file a mandatory report or to proceed with a transaction after being told a report needs to be filed
  - Customers making multiple online loan transactions in a manner that indicates structuring
  - Frequent overpayment of loan repayments
  - Customer frequently changes linked external bank account details, in particular when followed by funds depletion in full or close to 95% of available balance
  - Loans are made for, or are paid on behalf of, a third party with no reasonable explanation

Best Practices – Red Flags

- Transactions
  - Borrower is reluctant to provide information necessary for lender to file a mandatory report or to proceed with a transaction after being told a report needs to be filed
  - Customers making multiple online loan transactions in a manner that indicates structuring
  - Frequent overpayment of loan repayments
  - Customer frequently changes linked external bank account details, in particular when followed by funds depletion in full or close to 95% of available balance
  - Loans are made for, or are paid on behalf of, a third party with no reasonable explanation

Questions/Discussion

If you would like to ask a question, you can ASK or type your question into the CHAT feature NOW.

Andrew E. Bigart
Partner
Venable LLP

aebigart@Venable.com
202.344.4323

Preston H. Neel
Partner
Bradley Arant Boult Cummings LLP

pneel@bradley.com
205.521.8491

Online Lenders Alliance