AML Risks in Wealth Management

Presentation to FIRMA

May 8, 2019

Robert J. Rhatigan | Orlando, FL

Dechert LLP

Overview

- This presentation covers:
  - Background on the AML regulatory regime
  - Role of regulators and law enforcement
  - Principal AML requirements and impact on wealth management
  - In-depth look at the CDD Rule
  - 2018 AML overview
  - Money laundering risks in the U.S. financial system
  - Recent enforcement trends
  - Questions

Background on AML Regulation

- Bank Secrecy Act of 1970 (BSA)
  - Currency and Foreign Transactions Reporting Act
  - Principal focus: maintenance of records and preventing tax evasion
  - Foundation for subsequent AML laws, most recently culminating with the USA PATRIOT Act of 2001
- For over 25 years, the BSA is principally applied to banks — later, broker-dealers, MSBs and other financial institutions

Role of Regulators

- Financial Crimes Enforcement Network (FinCEN)
  - Treasury department agency charged with administering and enforcing the BSA
- Federal Financial Regulators
  - FinCEN delegates inspection and examination authority to the federal financial regulators (OCC, FDIC, Federal Reserve, SEC, CFTC and IRS)
  - FFIEC Bank Secrecy Act / AML Exam Manual
- Certain regulators are charged with jointly adopting rules with FinCEN, but FinCEN retains primary regulatory authority

BSA Enforcement

- FinCEN retains authority to enforce violations of the BSA
- However, other federal agencies have asserted their own authority to enforce BSA requirements
  - Banking regulators: unsafe and unsound practices
  - SEC: Exchange Act Rule 17a-8 incorporates the BSA into the SEC's regulatory framework for broker-dealers
- Department of Justice
  - Prosecutes criminal violations of the BSA

AML Programs

- Each financial institution must adopt an AML compliance program:
  - Policies, procedures and controls reasonably designed to achieve compliance with the BSA and prevent the financial institution from being used for money laundering or terrorist financing
  - Appropriate customer due diligence (CDD) procedures
  - Designation of AML compliance officer(s)
  - Training for appropriate employees
  - Annual independent review to test compliance

Key Components of AML Program

- Risk Identification
  - Does the program identify current and emerging risks?
- Risk Mitigation
  - Does the program take steps to appropriately mitigate those risks?
- Governance
  - Does the program include an appropriate function for overseeing the effectiveness and implementation of the program?

Know Your Customer (KYC)

- Financial institutions are required to verify the identity of new "customers" under the Customer Identification Program (CIP) rule
- Financial institutions must verify the identity of individual beneficial owners of legal entity customers
  - Verification of identity is required, not verification of beneficial owner status
- Financial institutions are required to conduct due diligence on both the financial institution and its customer if it accepts a "correspondent account" for a non-U.S. financial institution

Importance of KYC

- KYC is central to the “risk identification” component of an effective AML program
  - Who is the client?
  - Who are the underlying beneficial owners?
  - What is the purpose of the relationship?
  - Is the client a PEP or associated with PEPs?

Suspicious Activity Reports (SARs)

- Financial institutions must file a SAR if they know, suspect or have reason to suspect that a transaction is unlawful or unusual
  - Must be filed if a transaction has “no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in”
- Financial institutions are not permitted to “tip” that they have filed a SAR
- Financial institutions enjoy a broad safe harbor from liability when filing a SAR

Importance of SARs

- SARs, and monitoring for SARs, are central to the “risk mitigation” component of an AML program
  - Does the client’s activity make business sense?
  - Is the client’s activity consistent with expected activity, based on KYC record?
  - If connected to a PEP, does the client’s activity appear related to public corruption?
- Challenge: Monitoring for the “known unknown”

Other BSA/AML Provisions

- ***Information Sharing*** – Financial institutions must respond to FinCEN requests for information about named suspects involved in ongoing criminal or investigative proceedings
- ***Primary Money Laundering Concern*** – Financial institutions must take action in response to FinCEN designations of "primary money laundering concern"
- ***Currency Reports*** – Financial institutions must report transactions in excess of $10,000 involving cash and certain other monetary instruments
- ***FBAR*** – Financial institutions must report financial interests in non-U.S. financial accounts
- ***Funds Transmittals*** – Financial institutions must maintain records of funds transmittals

Criminal Money Laundering Laws

- Generally unlawful to engage in a financial transaction involving the proceeds of certain crimes in order to conceal the nature, source or ownership of proceeds they produced
  - Specified Crimes – broad
  - Intent: willful blindness
- Financial institutions and service providers have been held liable for “willful blindness” to the money laundering activities of its customers

Importance of Criminal Money Laundering Laws

- Even if an entity is not regulated under the BSA (such as a registered investment adviser), the entity is required to comply with criminal money laundering laws
- Entities that engage in illicit transactions and are “willfully blind” to such activities may be criminally liable.

CDD Rule – New Fifth Pillar for Covered Financial Institutions

- **Four Pillars** - Each financial institution must adopt an AML compliance program that includes:
  1. Policies, procedures and controls reasonably designed to achieve compliance with the BSA and to prevent the financial institution from being used for money laundering or terrorist financing
  2. Annual independent testing for compliance
  3. Designation of AML compliance officer(s)
  4. Training for appropriate employees
- **Fifth Pillar –** CDD Rule requires covered financial institutions to include in their AML compliance programs:
  5. Appropriate risk-based CDD procedures, including:
     i. Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile and
     ii. Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information

  Covered financial institutions include: federally regulated banks and federally insured credit unions, mutual funds, broker-dealers, FCMs and introducing brokers in commodities

Key Components of CDD Program

- FinCEN described the key elements of a CDD Program to include:
  - Identifying and verifying the identity of customers (CIP Program)
  - Identifying and verifying the identity of beneficial owners of legal entity customers
  - Understanding the nature and purpose of customer relationships and
  - Conducting ongoing monitoring

Beneficial Ownership Requirements

- General requirement:
  - Identification
    - Identify the beneficial owner(s) of each legal entity customer at the time a new account is opened, unless the customer is otherwise excluded or the account is exempted
    - Information required to be collected includes: (i) name and title of person opening the account; (ii) name and address of the legal entity; (iii) and the following information for each beneficial owner and control person: name, date of birth, address, SSN (U.S. persons) or passport number or other similar identification number (foreign persons)
  - Verification
    - Verify the identity of each beneficial owner through risk-based procedures
    - Procedures may be the same as CIP procedures
    - Do not need to verify the status as beneficial owners, only their identity

Beneficial Ownership Requirements (cont.) - Definitions

- What is a legal entity customer?
  - Any corporation, LLC, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an ***account***.
  - "Account" has the same meaning as in the CIP rules
    - E.g., for banks – a formal banking relationship established to provide or engage in services, dealings, or other financial transactions
- Who is a beneficial owner?
  - Each individual who directly or indirectly owns 25% or more of the equity interests of a legal entity customer; and
  - A single individual with responsibility to control, manage, or direct a legal entity customer (e.g., CEO, CFO, COO, managing member or GP)

Beneficial Ownership Requirements (cont.) - Exclusions

- There are a number of exclusions from the definition of legal entity customer, including (but not limited to):
  - Financial institution regulated by a Federal functional regulator
  - Registered investment company
  - Registered investment adviser, exchange or clearing agency, and any other entity registered with the SEC under the Securities Exchange Act of 1934 (e.g., broker-dealers)
  - CPO, CTA, SD and MSP
  - Bank Holding Company
  - Insurance company
  - Pooled investment vehicle operated or advised by a financial institution that is excluded from the definition of legal entity customer
  - Foreign financial institution established in a jurisdiction where its regulator maintains beneficial ownership information of the institution

2018 AML Overview

- U.S. Treasury published its National Illicit Finance Strategy and Supporting Risk Assessments, including the National Money Laundering Risk Assessment
- The CDD Rule became effective May 11, 2018
- FinCEN reaffirmed that virtual currency administrators and exchangers are MSBs that are required to register with FinCEN and have in place AML programs
- FATF updated its list of jurisdictions with AML/CFT deficiencies
  - Bahamas, Botswana and Ghana were added
  - Iraq and Vanuatu were removed
- Virtual currencies and marijuana related businesses continue to be a focus of regulators and law enforcement
- Interagency statement on sharing BSA resources

Money Laundering Risks in the U.S. Financial System Identified in 2018

- Money laundering risks and vulnerabilities identified by the U.S. Treasury in its 2018 risk assessment include:
  - U.S. currency remains one of the most widely used and accepted currencies worldwide
    - bulk cash smuggling
    - structuring transactions
    - funnel accounts
  - Rise of virtual currencies
    - Decentralized blockchain technology has been assisting law enforcement with tracking and uncovering criminal use of virtual currencies
    - The use of anonymity software and “altcoins” that provide more anonymity with respect to transaction records is growing among criminals
    - At some point virtual currency must be exchanged into fiat currency making virtual currency exchangers vulnerable to money laundering abuses
    - Virtual currency ATMs

Money Laundering Risks in the U.S. Financial System Identified in 2018 (cont.)

- Complex legal entities
  - Complex legal entities have been used to hide the identity of criminal beneficial owners or the illicit source of funds
  - Use of nominee owners, transactions between complex legal entity customers and cross-border transactions
  - Vulnerability may be mitigated with implementation of the CDD Rule (discussed below)
- Complicit merchants, professionals and employees of financial services companies
  - Merchants: black market currency exchanges (most common include peso and yuan exchanges)
  - Attorneys: use of IOLTA accounts
  - Real estate professionals: use of mortgage pay-offs and follow-up transactions
  - Financial services employees: bankers, MSB operators, broker-dealers and precious metals dealers
- Compliance deficiencies at banking organizations
  - –

Recent Enforcement Trends

- In 2018, U.S. regulators and law enforcement imposed close to $3 billion in fines and penalties for AML/sanctions violations.
- Key trends:
  - Multi agency actions
  - Personal liability for violations
    - Enforcement cases target AML compliance officers and senior executives
    - Merchants Bank: $311,000 in civil penalties against six current and senior executives and board members
    - Aegis Capital Corporation: senior executives were alleged to have aided and abetted the firm's failure to file SARs related to low-priced securities transactions
    - Chardan Capital Markets: AML Officer was alleged to have aided and abetted the firm's failure to file SARs related to transactions and did not investigate red flags related to low-priced securities transactions

Recent Enforcement Trends (cont.)

- Focus on misrepresentations/obstruction by financial institutions
  - February: Rabobank pled guilty to defrauding the OCC to obstruct its AML exam of the bank, forfeited over $350 million
- Failure to detect and/or report SARs
  - US Bancorp “capped” SAR filings; resulting in failure to report numerous SARs. UBS Financial Services, Inc. was alleged to have inadequate staffing that led to a back-log in SARs
  - Bank of China entered into consent order related to deficiencies in transaction monitoring systems resulting in the failure to timely file SARs
  - Central States Capital Markets (broker-dealer) was alleged to have willfully failed to file SARs in connection with the alleged illegal activities of one of its customers
  - Capital One, N.A., in part due to failure to comply with prior consent order related to weaknesses in BSA/AML compliance and failure to file SARs
  - Mega International Commercial Bank Co., Ltd. entered into a consent order relating to AML program deficiencies, including the failure to properly identify or report suspicious activities

For further information, visit our website at **dechert.com.**

Dechert
LLP