Anti-Money Laundering, Anti-Terrorist Financing & Compliance Challenges

Marc Cohen
Partner
+1 202 263 3206
mcohen@mayerbrown.com

Alicia Kinsey
Senior Associate
+1 202 263 3356
akinsey@mayerbrown.com

Stephanie Robinson
Partner
+1 202 263 3353
srobinson@mayerbrown.com

Financial Services Regulation
IN A POST DODD-FRANK WORLD
Anti-Money Laundering Developments

Alicia Kinsey
Senior Associate
+1 202 263 3356
akinsey@mayerbrown.com

Financial Services Regulation
IN A POST DODD-FRANK WORLD
Topics to be Discussed

• FinCEN:
  – Overview of Regulatory and Enforcement Developments
  – Customer Due Diligence Rule

• NYDFS Anti-Money Laundering (AML) and Sanctions Compliance Proposal
Recent FinCEN Regulatory Actions

- **August 2015** – Proposal to apply BSA requirements to registered investment advisers
- **January 2016** – Issuance of geographic targeting orders for cash real estate transactions in Miami and New York
- **March 2016** – Additional guidance on implementation of the prepaid access rule and relationship to CIP requirements
- **April 2016** – Proposal to apply BSA requirements to funding portals
FinCEN Enforcement Actions

• Four actions against casinos, two against MSBs, one each against private banks, precious metals dealers, and banks; generally focused on:
  – Lack of AML compliance program or culture of compliance
  – Failure to file CTRs and/or SARs
  – Involvement of senior management in non-compliance

• Withdrew PATRIOT Act § 311 designations against Liberty Reserve, JSC CredexBank, Banca Privada d’Andorra, and Lebanese Canadian Bank
  – Continuing litigation regarding designation of FBME Bank
• Four “pillars” of an Effective AML Compliance Program:
  – System of internal controls;
  – Independent testing;
  – Designated AML compliance officer; and
  – Training.

• Final CDD Rule released in May 2016
  – Effective July 11, 2016; compliance required by May 11, 2018
FinCEN: Customer Due Diligence Rule

• 5th Pillar—Customer Due Diligence (CDD)
  – 2012: FinCEN issued ANPR, followed by industry outreach
  – 2014: Proposed rule issued

• Four Core Requirements of CDD
  – Customer identification and verification
  – Beneficial ownership identification and verification
  – Development of a customer risk profile
  – Ongoing monitoring for suspicious transactions (and updating beneficial owner information on a risk basis based on monitoring)
• Beneficial owners are:
  – Generally, natural persons who own 25% or more of the legal entity or exercise significant management responsibility
  – “Ultimate” beneficial owners; not nominees or pass-through entities

• Final CDD rule is a “floor”; e.g.:
  – Financial institutions may require identification of less than 25% beneficial owners
  – Federal functional regulators may impose more extensive requirements
• The CDD requirement applies to accounts at financial institutions opened:
  – By legal entities (e.g., corporations, LLCs, partnerships); and
    • But not trusts, unincorporated associations, or sole proprietorships
  – On or after May 11, 2018
    • Existing customers exempted

• Financial institutions are defined as banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers
• Exemptions from beneficial ownership requirement:
  – Regulated US financial institutions (including US pooled investment vehicles);
  – Governments and governmental entities;
  – Publicly traded companies;
  – Non-US legal entities organized in a jurisdiction where a regulator maintains beneficial ownership information;
  – Non-profit organizations (only with respect to the 25% ownership prong); and
  – Entities opening private label retail credit accounts.
FinCEN CDD: Required Documentation

• Person opening account for the legal entity must complete a form certification (or equivalent) that lists:
  – Any natural persons owning 25% or more of legal entity’s equity
  – One person with “significant management responsibility”
    • May also be a 25% or greater owner
  – Is completed on a “best of knowledge” basis (as opposed to penalty of perjury)

• Financial institution must collect CIP information for all persons listed on the form certification
  – Consists of name, address, date of birth, and taxpayer ID
  – Documents verifying CIP information (e.g., driver’s license) may be photocopies
  – Purpose is to identify individual, not confirm status as a beneficial owner
• Financial institutions may rely on CDD compliance by other financial institutions
  – Same standard as CIP reliance for natural person customers

• Financial institutions do not need to:
  – Remediate existing accounts, unless other risk-factors indicate remediation is warranted; or
  – Update CDD information unless they know or suspect the information on file is inaccurate

• Additional compliance expected if there are red flags
  – FinCEN is “okay” with financial institutions that decide to gold plate their AML compliance programs
NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
AML & SANCTIONS
PROPOSAL
In December 2015, the NYDFS proposed new regulations (the “Proposal”) that would require regulated financial institutions to implement transaction monitoring and watch list filtering programs to ensure compliance with federal AML and sanctions laws.

Regulated financial institutions include:

- New York-chartered banks and trust companies;
- New York-licensed branches and agencies of foreign banks; and
- New York-licensed check cashers and money transmitters.

Proposal has not yet been finalized, but compliance may be required as early as 2017.
The Proposal would require regulated financial institutions to maintain a program for monitoring transactions:

- For potential BSA/AML violations and suspicious activity reporting
  - For reporting purposes
- That are prohibited under applicable sanctions programs, including OFAC sanctions, politically exposed persons (“PEPs”) lists and internal watch lists
  - For interdiction purposes

CCOs of regulated financial institutions would be required to submit an annual certification to NYDFS.
Regulated financial institutions would be expected to implement detailed procedures to comply with the Proposal, including:

- End-to-end, pre-and post-implementation testing of their compliance program;
- On-going analysis to assess the effectiveness of the institution’s compliance efforts;
- Investigative protocols on how to respond to alerts; and
- If third-party service providers are used comply with the Proposal, a vendor selection process to identify qualified outside consultants.

Regulated financial institutions would not be allowed to change or alter their compliance program in a manner that would lower or otherwise minimize their filing SARs.
SPARKS NUGGET CASINO
ENFORCEMENT ACTION
Sparks Nugget Casino Enforcement Action: Recognition of Compliance Officer’s Efforts

- In April 2016, FinCEN assessed a $1 million penalty on the Sparks Nugget casino for AML violations related to a systemic breakdown in its compliance program
  - Failed to file CTRs and SARs
  - Failed to maintain required records
  - Failed to implement and maintain an effective AML program

- FinCEN recognized that the casino’s single compliance manager attempted to address the violations, but that casino management:
  - Instructed the compliance manager not to communicate with IRS auditors;
  - Prevented the compliance manager from reviewing the IRS exam report;
  - Chose not to file SARs the compliance manager had drafted; and
  - Disregarded the compliance manager’s concerns regarding non-compliance.
Developing Issues for Compliance Officers

Stephanie Robinson
Partner
+1 202 263 3353
srobinson@mayerbrown.com

Financial Services Regulation
IN A POST DODD-FRANK WORLD
Topics to be Discussed

• Increased focus on the compliance function
  – Greater individual liability
  – Heightened government interest
  – More extensive reporting and coordination

• Best practices for compliance officers
  – Resources
  – Authority
  – Culture
  – Training and testing
INCREASED FOCUS ON THE COMPLIANCE FUNCTION
Greater Individual Liability

- Regulators and prosecutors have increasingly focused on the compliance function in bringing enforcement actions
  - Inadequate or ineffective compliance resources
  - Compliance function approved of culpable conduct

- Individual compliance officers are being:
  - Identified in corporate settlements
  - Pursued for individual liability
DOJ Yates Memorandum on Individual Accountability for Corporate Wrongdoing

• Perception that “bad actors” escaped prosecution for causing the financial crisis

• DOJ issued guidance in September 2015 that requires prosecutors to take steps to strengthen the DOJ’s pursuit of individual corporate wrongdoing in criminal and civil actions; prosecutors must:
  – Receive all relevant facts about individuals involved in corporate misconduct for the corporation to receive cooperation credit;
  – Focus on individual wrongdoing from the inception of an investigation;
  – Communicate with civil/criminal counterparts during a corporate investigation;
  – Absent extraordinary circumstances, not provide protection to individuals as part of the corporation’s resolution/settlement;
  – Develop a clear plan to pursue related individual cases (or document declinations) prior to settling with a corporation; and
  – Focus on individuals and the company in evaluating whether to bring suit and consider factors beyond an individual’s ability to pay a judgment
In December 2015, NYSDFS proposed new regulations that would require NY-chartered or licensed financial institutions to implement transaction monitoring and watch list filtering programs to ensure compliance with federal AML and sanctions laws.

Proposal requires an institution’s CCO to certify annually that:

- They have reviewed the institution’s transaction monitoring program and the watch list filtering program; and
- The institution complies with the requirements set out in the regulation.

Criminal penalty for filing an incorrect or false certification:

- Potential for strict liability against CCO.

CCOs may be concerned with receiving “waterfall” sub-certifications or relying on internal assurances of compliance:

- CCOs may lack managerial or budget authority to implement an appropriate compliance program or hire verification/testing consultants.
OCC Penalty Guidance

• In early 2016 the OCC issued:
  – An update to its civil money penalty matrix (how examiners determine the penalty for compliance failures)
  – A guide for how the agency will determine punishments for BSA/AML failures

• Revised matrix focuses on remediation of violations to receive positive credit

• Guide requires examiners to issue an enforcement action for long-running, uncorrected AML compliance failures
  – Not as severe as the NYS DFS proposal’s individual liability, but CCOs may be subject to penalties for deliberate violations or obstruction of the agency’s investigation/examination
FinCEN v. Haider

• In December 2014, FinCEN sued the former CCO of a large money-services business (MSB) for failing to:
  – Implement an effective AML program; and
  – Fulfill its suspicious activity reporting (SAR) obligation

• Alleged culpable conduct included the failure to (i) implement a discipline policy, (ii) terminate high-risk agents/outlets, (iii) file timely SARs, (iv) conduct effective agent/outlet audits, and (v) conduct adequate agent/outlet due diligence

• FinCEN sought a $1 million civil money penalty and a ban from the industry
  – MSB separately settled with the government for permitting its network to be used for fraudulent transactions
  – Is the first ever FinCEN lawsuit against a CCO

• In January 2016, the district court held that individual officers of financial institutions may be liable for the failure of an institution’s AML program
  – Because the court denied the motion to dismiss, the suit will continue
SEC Actions Against CCOs

• In April 2015, the SEC took an enforcement action against a broker-dealer’s CCO for failing to report a material compliance matter to the BD’s board.

• In June 2015, SEC Commissioner Aguilar noted that CCOs who “strive to do their jobs competently, diligently, and in good faith . . . should have nothing to fear from the SEC.”

• In November 2015, the SEC’s examination office released guidance for advisers and funds that outsource CCO duties should:
  – Be empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the firm; and
  – Have a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

• In November 2015, the head of the SEC’s Enforcement division announced that the agency would bring cases against CCOs who:
  – Engage in affirmative misconduct or obstruct regulators (generally dual-hatted employees)
  – Exhibit wholesale failures to carrying out compliance obligations.
More Extensive Reporting and Coordination Relationships

• Modern CCOs are expected to report not only to senior management, but also to the board of directors
  – Trend of standalone compliance department that is separate from legal and business lines
  – Model of compliance as a second line of defense (between the front line business unit and the internal/external audit function)

• CCOs of regulated entities are expected to engage with examiners

• CCOs must coordinate compliance efforts with legal, internal and external audit, and risk management
BEST PRACTICES FOR COMPLIANCE OFFICERS
Sufficient Resources

• CCOs must ensure that the compliance function receive sufficient resources to perform its duties
  - Resources may include technical capabilities (i.e., detection software), as well as human capital
  - Compliance resources should be separate from internal audit, risk management, legal, and business line resources
  - Resource allocation should be consistent with the entity’s risk assessment, and should target areas/activities with the high risk/cost of non-compliance
Independent Authority

• CCOs should have appropriate authority to identify and remediate problems, including:
  – Direct communication with senior management, external auditors, regulators, and the board (or an appropriate committee of the board);
  – Access to all data and personnel;
  – The ability to reject or “fire” problematic customers, employees, and product offerings; and
  – Clearly documented procedures for resolving disagreements with business lines.
Culture of Compliance

• CCOs need support from management, including senior management and the board; management should:
  – Subject its own activities to review by compliance;
  – Participate in compliance training;
  – Refuse to tolerate non-compliance, even by profitable employees;
  – Communicate that compliance with law and company policy is required to retain employment and/or bonuses; and
  – Ensure that compliance concerns or instructions receive appropriate attention from business line personnel.
Training and Testing

• Employees must receive training on the importance of compliance; all employees should be able to:
  – Identify conduct in their unit that does not comply with relevant law or company policy;
  – Report potential non-compliance without fear of retaliation; and
  – Show completion of compliance training.

• Companies must engage in testing of their systems, including compliance systems; testing should be:
  – Independent (internal or external);
  – Reflective of current industry practices;
  – Updated to include new industry practices;
  – Used by compliance and management to enhance operations going forward; and
  – Documented and disclosed to regulators (as appropriate).
Other Practices

• CCOs may wish to consider implementing other best practices, such as:
  – Establishing standing meetings with regulators and external auditors to address concerns;
  – Participating in industry groups (e.g., FS-ISAC) to identify new compliance issues and techniques;
  – Implementing internal whistleblower reward and/or protection programs;
  – Periodic rotation of compliance personnel among business lines and the main compliance group; and
  – Retaining independent outside counsel to advise on conflicts with legal or business lines.
Anti-Terrorism Act Litigation:
WHY IT IS A RISK TO YOUR ORGANIZATION, AND HOW TO MINIMIZE THE RISK

Marc R. Cohen
Partner
+1 202 263 3206
alakatos@mayerbrown.com
The Problem

• Difficult to obtain compensation from terrorists because they are hard to identify and locate, and likely are “judgment proof”

• Prosecutorial resources focused on:
  – Stopping attackers and deterring would-be attackers
  – Shutting down direct financial donors and charities
The Solution

• Target “financial angels” because money is the “lifeblood” of terrorism
  – OFAC sanctions model

• American victims of terrorism as private attorneys general
  – RICO model: treble damages and attorneys’ fees
  – Sections 1983 and 1988 (civil rights model): attorneys’ fees
Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism . . . may sue therefor . . . and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney’s fees.” 18 U.S.C. § 2333.

- Modeled on RICO
- Covers terrorist financing
Unintended Consequences

• Policy dictated by persons with financial interest, rather than legislative judgment and prosecutorial discretion

• Fiscal incentive for overreaching lawsuits
  – RICO has been used more against business people than organized crime
• ATA suits not limited to terrorists
  – Banks that merely transferred funds
  – Twitter because ISIS uses it to communicate
• Definition of “international terrorism” stretched passed breaking point
  – Cartel-on-cartel violence (Zapata)
• Causation weakened
  – “Money is fungible” Boim.
Scorecard

• Plaintiff losses
  – *Rothstein v. UBS*: Causation respected

• Plaintiff victories
  – *Weiss v. NatWest*: UK determination that NatWest’s client was not linked to terrorism was not dispositive
  – *Goldstein v. Arab Bank*: Jury verdict on liability, then settlement before damages phase

• Some cases settled
Plaintiffs’ Arsenal

• Sympathetic clients v. negative public views toward banks
• Reluctance of judges, legislators to be seen as “soft” on terrorism
  – Statute of limitations increased to 10 years
• Mere allegations cause reputational issue
• Bank secrecy / data protection laws limit discovery responses
  – Harsh sanctions v. Arab Bank
• Strong preference for U.S. forum
Preemptive Defense

- Strong AML and anti-terrorist finance compliance enforcement and culture
  - Consider global compliance policy
  - Act on negative news, myriad sanctions lists

- De-risking
  - Charities may be high risk

- Limit on-boarding
Legislative Actions

• Proposed legislation adding an “aiding and abetting” provision to the ATA is pending
  – Would make early dismissal more difficult and increase proliferation of ATA suits

• Trade groups have proposed language carving out innocent financial institutions
  – Your support may help