Strengthening Compliance Oversight with a Risk-based Approach & Dealing with Cybercrime

Seminar on PMLA

25th March 2017

Reporting Entities

- Banking Company
- Financial Institution
- Intermediary or a person carrying on designated business or profession

Persons carrying on Designated Business or Profession

- *a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino*
- *a Registrar or Sub-Registrar appointed under Section 6 of the Registration Act, 1908, as may be notified by the Central Government*
- *real estate agent, as may be notified by the Central Government*
- *dealer in precious metals, precious stones and other high value goods, as may be notified by the Central Government*
- *person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government*
- *person carrying on such other activities as the Central Government may, by notification, so designate, from time to time*

Obligations of Reporting Entity

- have to maintain a record of all transactions covered as per the nature and value of which may be prescribed
- enable it to reconstruct individual transactions
- furnish to the Director (FIU) within such time as may be prescribed information relating to such transactions,
- whether attempted or executed
- verify the identity of its clients
- identify the beneficial owner, if any, of such of its clients
- shall maintain record of documents evidencing identity of its clients and beneficial owners
- shall maintain the same for a period of five years after the business relationship

Compliance

Placement | Layering | integration

- Clients
- Beneficiaries

- All Transactions
- Prescribed Value
- Nature

- Attempted
- Executed

- Documents
- Trails
- 5 years

- Director (FIU)

Challenges

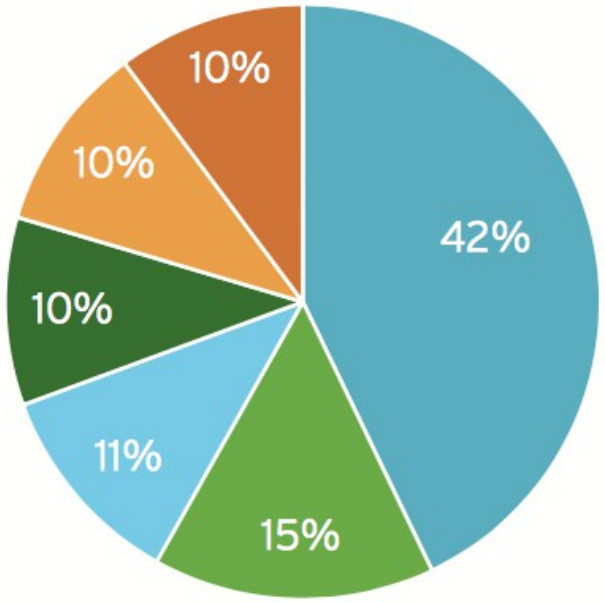
- Absence of automation across the entire information flow channel
- Manual Intervention at every step
- Islands of information processing systems
- Parameters incorrectly configured
- Collusion
- International – Multiple entities across multiple nations
- Co-operation amongst agencies not cordial
- Investigating Methods and tools used disparate and deduce differing results

Integrated and Unified Approach to risk mitigation and compliance

- ***Conduct a risk assessment*** *based on the products, services, geographies and clients to better understand the threat environment*

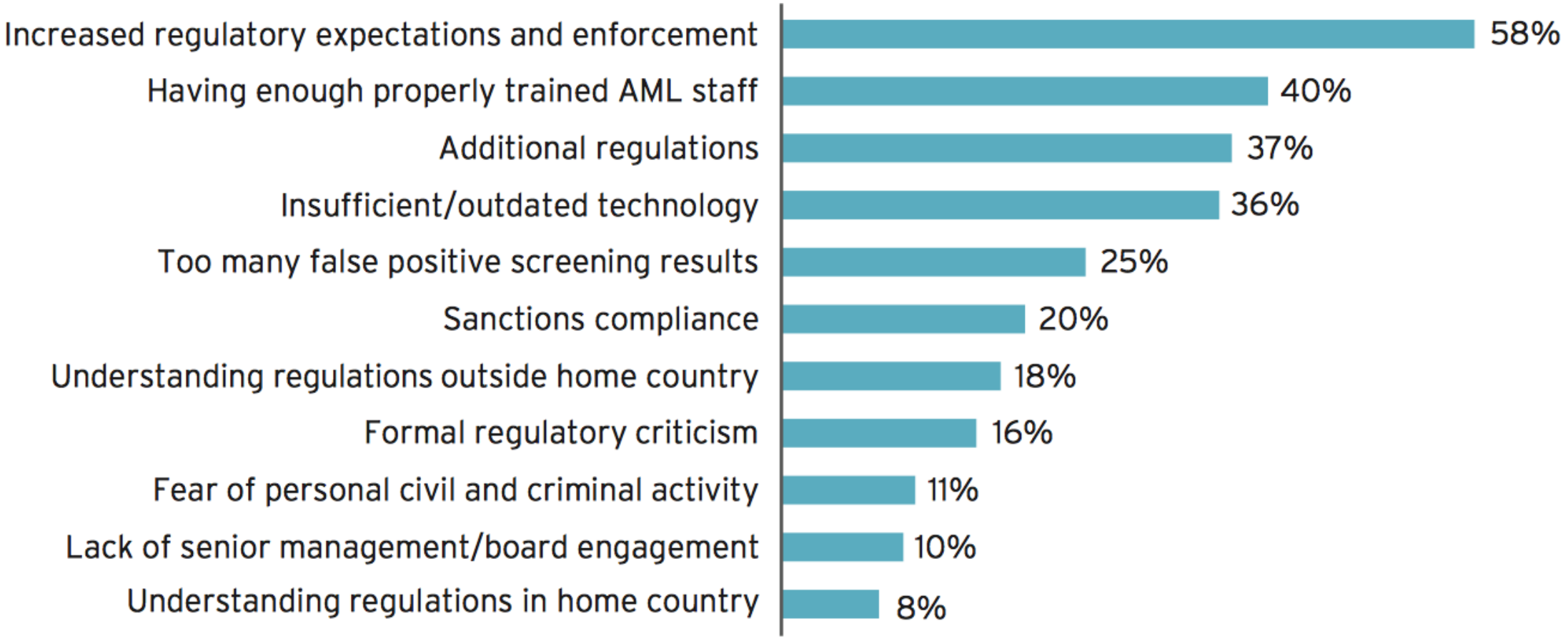
The Need for Change

- Rising Threats
  - *A number of drivers — including globalization, the proliferation of banking channels, rising transaction volumes and accelerated technology advancements (i.e., new digital tools and intelligent automation) have introduced new opportunities for financial malfeasance*
- Heightened Regulatory Scrutiny and Surging Compliance Costs
  - *Regulators across the globe have intensified their scrutiny and are assessing heavy fines to Reporting Entity's that fail to adopt adequate defenses or that violate the Banking Secrecy Act/Anti-Money Laundering (BSA/AML) program. Between 2007 and 2014, Reporting Entity's paid about $21 billion in cumulative anti-money laundering (AML) fines alone in the U.S.*



- Evolving criminal methodologies
- Cost of AML compliance
- Lack of personnel in risk function
- Civil prosecution/class actions
- Geo-political events
- Sectoral sanctions

AML Compliance Challenges in the Next 12 Months



Why Heavy Investment Still Feels Short Change

- Invested heavily in strengthening security and meeting compliance demands,
  - *but such efforts are undermined by their piecemeal approach to dealing with financial crime.*
  - *Risks such as money laundering, cyber- crime and fraud are traditionally handled independently by various organizational functions.*
  - *Each has its own tools, systems, processes and compliance mechanisms, with minimal communication among them*
- This fragmented approach has resulted in duplication of data, technology and efforts, resulting in rising costs

Major Fines Applied to Foreign Banks for U.S. Sanctions Law Violations

Bank	Year	Fine (in $ million)
BNP Paribas (France)	2014	8900
Standard Chartered (UK)	2013	667
ING (The Netherlands)	2012	619
Credit Suisse (Switzerland)	2009	536
ABN Amro (The Netherlands/UK)	2010	500
HSBC (UK)	2012	375
Lloyd's (UK)	2009	350
Commerzbank (Germany)	2015	342
Bank of Tokyo – Mitsubishi (Japan)	2014	315
Barclays (UK)	2010	298
Deutsche Bank (Germany)	2015	258
Bank of Tokyo – Mitsubishi (Japan)	2013	250
Clearstream (Luxembourg)	2014	152
Royal Bank of Scotland (UK)	2013	100

Tailor the Risk Management Approach

- *The key to developing and applying adequate controls is becoming knowledgeable about the risks themselves and the business areas they impact.*
- *A risk assessment should then be carried out based on the organization’s size, channels, geographies, customer types and product and service complexity (e.g., risks for wealth management products can arise from high-value transactions, politically connected individuals, multiple jurisdictions and banking secrecy).*
- *By mapping these risks against internal policies, procedures and controls, Reporting Entity's can assess their effectiveness in mitigating risks, and ne-tune them accordingly.*
- *A periodic review of the risk assessment should be conducted to ensure relevancy.*

Address Silos

- *There is a wide spectrum of financial crime types, including money laundering, terrorist financing, fraud and cyberattacks.*
- *Intrusions, however, often go unnoticed, as these disciplines often operate in silos.*
- *To more effectively manage the growing sophistication of crimes, Reporting Entity's are increasingly focused on tightly integrating or merging the various internal functions tasked with financial crime prevention.*
- *However, some experts warn about the risks of such integration as it can increase vulnerability to cyberattacks, and instead recommend improving communication and coordination among the teams*
- *start by integrating transaction monitoring in their cybercrime and AML disciplines*

Start by integrating transaction monitoring

- For example, if a cyberattack occurs that involves the theft of online customer data,
  the team within the AML discipline could provide complete details of all suspicious activities tagged by its transaction monitoring systems.
- These details could then be used to cross-check any surge in e-commerce purchases, wire transfers, ATM withdrawals or similar transactions, thus detecting and preventing criminals from using the stolen data
- Similarly, a cyberattack alert by the cybersecurity team will enable the AML function to tighten transaction scrutiny and prevent money laundering, while the fraud prevention team can take steps to ensure the stolen customer data is not monetized, as well as investigate insider activity.
- The sooner the information is passed to the other teams, the more time they have to prevent the crime or identify the perpetrators

Overcome Data Challenges

- The key to integrating multiple risk efforts lies in the bank’s ability to get high-quality and consistent data from across the organization
- This is no easy task for large Reporting Entity's, many of which have accumulated multiple systems and technologies over the years through mergers and acquisitions
- Standardizing large volumes of customer, trans- action, crime and other unstructured and semi- structured data from across the organization can be a challenge, as is encouraging employees to comply with internal standards and practices when entering data
- Doing so can signicantly improve the overall data quality and accuracy needed to support real-time monitoring and data-driven decision-making

Embrace Analytics

- Combining effective data management with advanced analytics is essential for detecting and preventing growing threats
- By collecting and analyzing the massive volumes of current and historic data within the organization (across all lines of business) and from external agencies providing financial crime data, Reporting Entity's can gain a comprehensive view of customers and transactions, as well as insights into relationships between various entities that previously went unnoticed
- Through analytics, Reporting Entity's can better understand the risks posed by customers, transactions and other entities, and discover complex threats that impact multiple lines of business.

Embrace Analytics ..

- For instance, a transaction that appears legitimate in one channel may appear suspicious when viewed holistically.
- Forensic data analytics will help Reporting Entity's identify and predict risk patterns and issues in advance, enabling them to pre-empt criminal activity, particularly insider threats and data breaches that involve gaining unauthorized access to sensitive data.

Address Culture and People Challenges

- The tone set by senior management is key to driving an organization’s crusade against financial crime.
- Senior bank of officials need to set account- ability standards, establish policies and controls, promote transparency by working closely with regulators, provide incentives for promoting compliance, and show zero tolerance toward potential internal and external risks
- Organizations should also grow their awareness of emerging threats, such as risks posed by virtual currencies and new channels and technologies
- Employees should be trained and updated on the latest regulatory developments and emerging risks, and be sensitized to the various ways criminals can exploit them
- High-risk users, such as contractors, suppliers and employees with access to sensitive organizational data and information, must be monitored and analyzed continuously for suspicious behavior or use of technology

Collaborate with Industry-wide Initiatives

- While Reporting Entity's have invested heavily to improve their compliance programs, evolving regulations have hindered them from developing a sustain-able and scalable solution
- Individual Reporting Entity's have developed proprietary solutions, with no industry- wide standards or best practices to guide them, resulting in duplicate efforts across the industry and accelerating compliance costs
- Reporting Entity's need to move toward a more collaborative and unified approach, similar to what exists for international trade confirmation and settlement. Doing so would address skill shortages, facilitate the creation of standards and best practices and foster innovation
- By collaborating with law enforcement agencies and the government, Reporting Entity's can also
  take the fight against financial crime to the next level

Collaborate with Industry-wide Initiatives ..

- A case in point is the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) initiative, a one-year pilot started in February 2015 by the government, Reporting Entity's, law enforcement agencies and others. The task force, expected to become a permanent institution, was set up to study the scale and methods employed in money laundering, suggest remedial measures and improve intelligence-sharing across parties

Looking Forward

- Fast-evolving financial crime and regulatory uncertainty impacts Reporting Entity's of all sizes and warrants a proactive approach. Large Reporting Entity's with multiple lines of business must focus on integrating various crime prevention disciplines and building a culture that supports data-driven decision-making. Reporting Entity's should consider hiring former military and law enforcement intelligence of officers with expertise in analytics to proactively identify trends in transactions with links to terrorist organizations.
- Small Reporting Entity's can seek technology and talent resources from businesses that specialize in cybercrime to avoid the high costs of procuring, maintaining and updating technology, as well as attracting and retaining people with needed skills, while also gaining the flexibility to offer new products and services and enter new business areas. This is signicant as small Reporting Entity's are beginning to adopt new business lines or product segments that larger Reporting Entity's have exited due to higher BSA/ AML compliance risks

Approach to Combating Cyber Crime

- Use threat modeling

- Other strategies to help thwart increasingly sophisticated cyber attacks.

Benefits of a risk-based approach

- Develop a more in-depth understanding of an IT environment, and of its strengths and vulnerabilities.
- Accrue actionable risk intelligence
- Define the value and risk-related significance of categories of data, and prioritize and protect them accordingly
- Analyze previous security incidents to identify “lessons learned”
- Identify customers, suppliers, service providers, and other parties that have compromised devices inside their networks
- Analyze malicious code on compromised machines to develop cyber intelligence.
- Track compromised data that has left or is leaving the organization
- Understand the organization’s susceptibility to persistent, sustained access by cyber criminals

Balancing present and future needs.

- Plan for future innovations with cyber risk management in mind.
- Improve agility by implementing new security protocols and other changes in short sprints.
- Focus on pacing and monitoring to keep everyone working toward the same goal.
- Create a team to bring security initiatives to each line of business via in-person briefings, emails, and phone calls.
- Move cyber risk management directly into strategic and tactical planning.

Investing wisely

- Evaluate the spending impact of any potential new solutions.
- Gather enough resources to implement them effectively.
- Hire personnel required to execute plans.
- Invest in customer and employee cyber risk training.
- Allocate budget not just in IT but across the enterprise, including operations and infrastructure, application development, and human capital.

Getting the right talent

- Look beyond FSIs when building teams. It may be easier to train newcomers for industry knowledge than for tech skills, so recruit for the latter. Those with backgrounds in military and government intelligence can often be a particularly good fit.
- Exercise strong onboarding routines when hiring from outside the industry to shorten the learning curve for outsiders

Lining up the right tools

- Seek out integrated solutions that reduce the headache of adding tools.
- Look nationally and globally: Silicon Valley and Israel each boast an abundance of innovative cyber startups.
- Consider implementing cyber risk managers for each line of business—one company slashed critical risks by 86 percent with this model.

Reporting results

- Take an enterprisewide view when assessing vulnerabilities, and don’t overreact to new threats in the news.
- Shift the reporting focus from the number of attacks to the degree of penetration and response time.
- Collaborate within the industry and beyond to set the bar for cyber risk management, support wider standardization efforts, and align on effective approaches.

Sharing cyber risk intelligence

- Foster trust with cybersecurity colleagues from other firms within the industry and beyond.
- Focus on quality rather than quantity of information, paying particular attention to action-based response intelligence.
- Work toward improved analytics and automation of threat intelligence assessments.

Questions ?

Thank You