Fintelekt®

AML Process Maturity- Nepal Banking Industry

Shirish Pathak
MANAGING DIRECTOR

January 27, 2017
kathmandu

AML Process Maturity Survey 2017

Participation
Compliance officers from 23 commercial and development banks

Objective
To assess the regulatory environment in Nepal and benchmark AML processes among banks

Coverage
Compliance officers' opinions on current challenges, organisational priorities, technology, processes, FIU & regulatory involvement

Key Overall Findings

Governance

- All banks have an AML/CFT policy in place, which is reviewed regularly
- 75% of the banks send quarterly reports to Board members

Risk Identification and Assessment

- 47% banks have updated high-risk customer profiles in the last 6 months
- 72% banks undertake periodic review of suspicious transactions as a potential risk management tool

Pillars of a sustainable AML compliance environment

Training

- AML training is provided to all front-line and compliance staff at least once a year at all banks
- 75% banks test the knowledge of their staff on AML/CFT

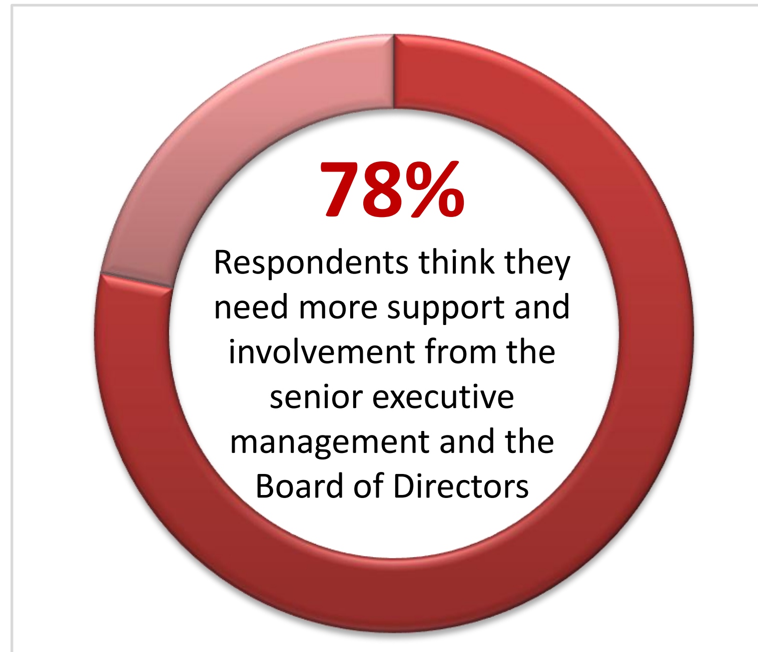
Technology

- 86% compliance officers regard procuring or enhancing their transaction monitoring system as their top priority in the next 1-2 years

AML compliance is considered a specialised function and an integral part of the organisation, according to all participating compliance officers

Key Concerns - Governance

- Compliance officers at 75% banks **send quarterly AML reports** to the Board of Directors
- However, 40% compliance officers felt that more efforts are required to **internally promote the organisational AML policy**
- 68% compliance officers consider the budget allocated to their department as ‘**nominal**’



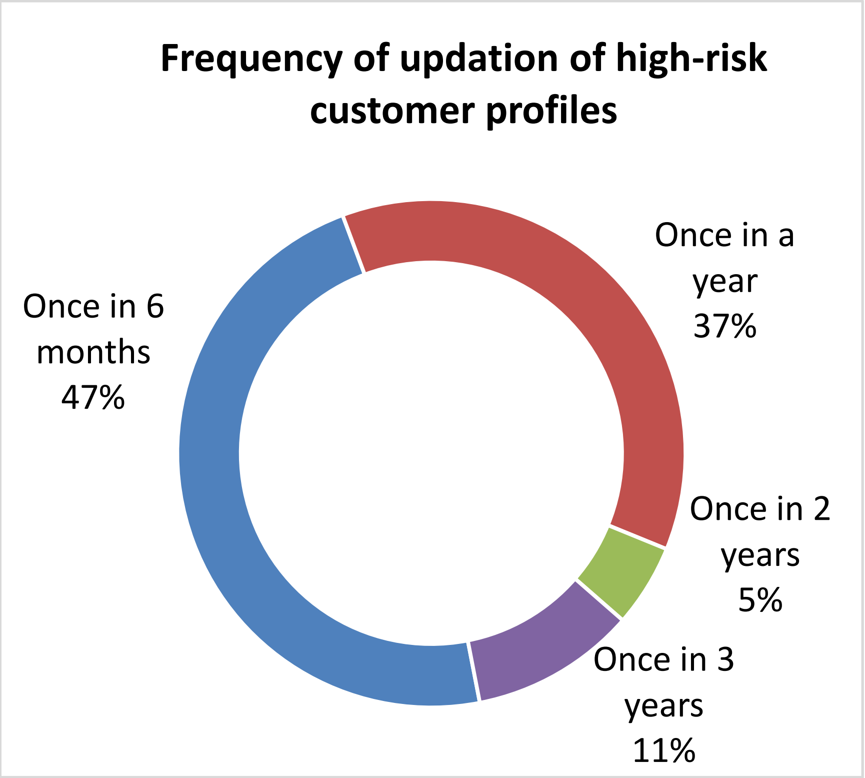
Stronger frameworks for continuous interaction and monitoring, driven by the top management, will provide the necessary priority to AML compliance

Key Concerns - Risk Identification and Assessment

40% banks have **never renewed** or have not renewed **low-risk customer profiles** in the last three years

35% banks have never undertaken an **organisation-wide AML/CFT risk assessment**

Only 41% banks are **reviewing money laundering risks** at every transaction



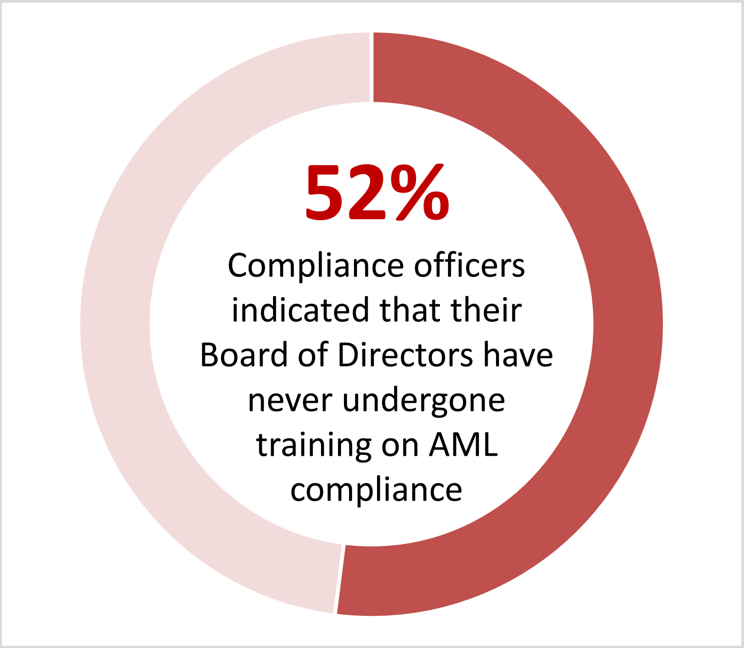
Up-to-date risk assessments will ensure banks are working with current typologies, and reduce the risk of regulatory penalties

Fintelekt®

Key Concerns - Training

Training is provided to **front-line and compliance staff** at least once a year in most banks

40% banks **do not provide role-specific training** tailored to the profile of the employee



Given that banks are relying on employee-generated triggers and alerts, training needs to take centre-stage to ensure employees are made aware of the latest threats

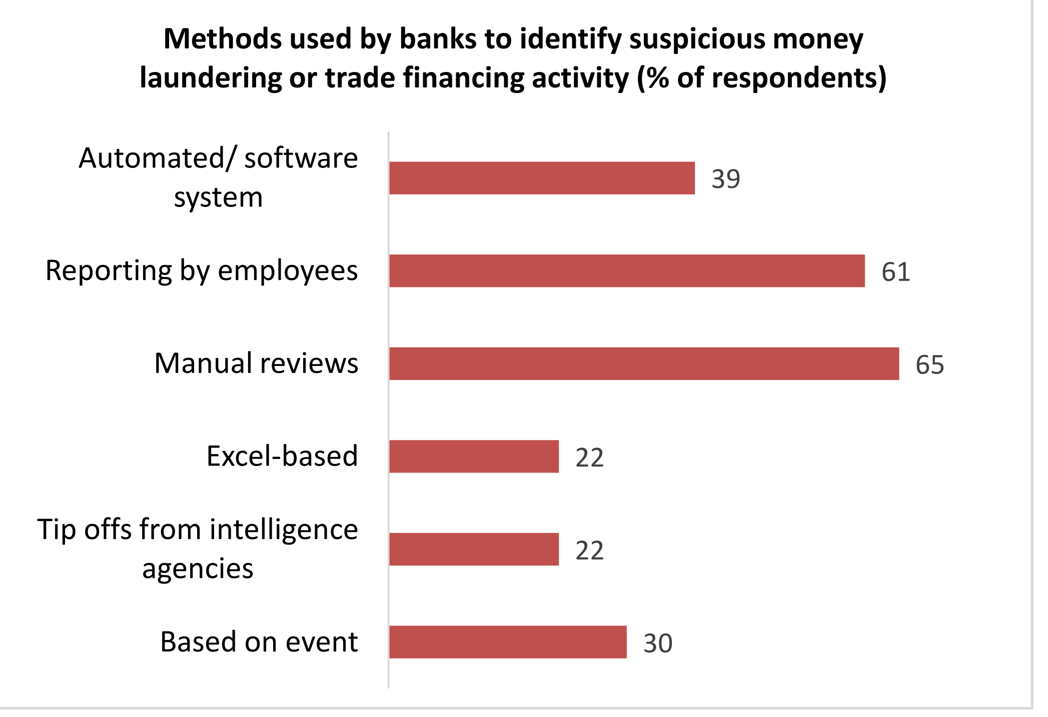
Fintelekt®

Key Concerns - Technology

47% of the banks **maintain KYC/ CDD records manually**

70% of the banks **do not have a system** which generates pop-ups or alerts automatically

86% compliance officers regard **procuring / enhancing their transaction monitoring system** to be the top most priority area in the next 1-2 years



Technology and automation requires supporting investment in training and processes

Way forward - Banks

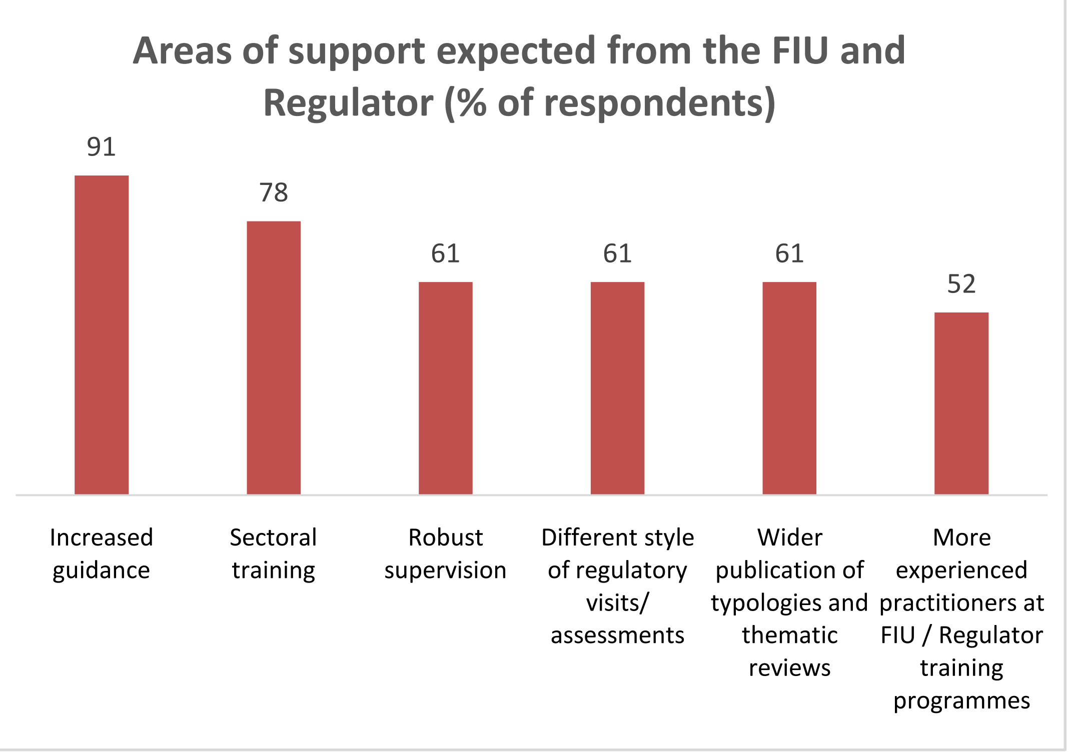
- Framework for continuous interaction between compliance staff and top management
- Specialised training for senior executive management team and Board members; role based training for other employees
- On-going risk assessments with respect to customers, products, services, entities, locations
- Investment in technology and automation

Investing in people, processes and technology today can contribute to a mature AML environment in future

Fintelekt®

Way Forward – FIU/Regulator

- **Capacity building** in terms of a robust technology platform, as well as human capital
- **Phased outreach and awareness programmes** for continued learning and sharing of best practices
- **Hand-holding reporting entities** and helping them arrive at a common understanding of suspicious transactions



A collaborative and incremental approach can lay the foundation of a stronger AML environment within the country

Fintelekt®

Research | Consulting | Events | Training

Shirish@fintelekt.com

THANK YOU

Trade Based Money Laundering

Presentation by

Jairam Manglani
Country Head of Financial Crime Compliance
Standard Chartered Bank, India

Trade & Trade Based Money Laundering (TBML)

- **Trade** can be simply defined as *"An act which involves the transfer of the ownership of goods or services from one person or entity to another in exchange for other goods or services or for money'.*

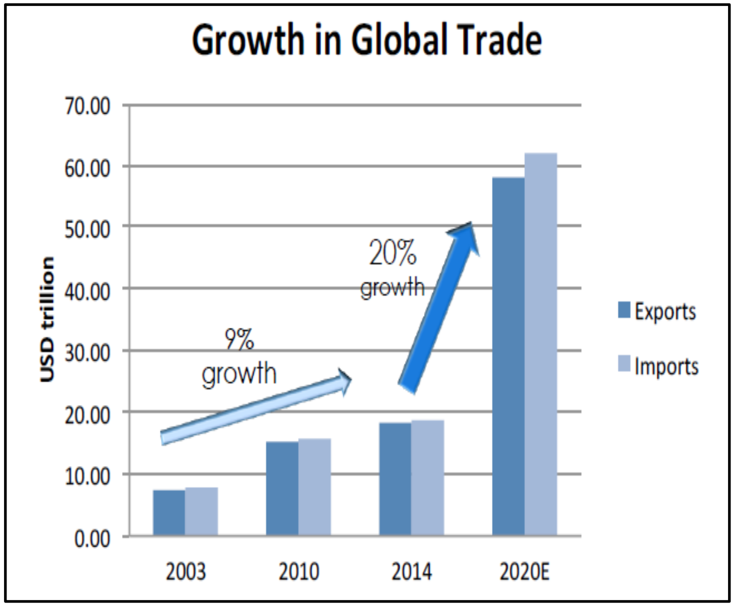
- The FATF Paper on Best Practices on TBML (2008) states:

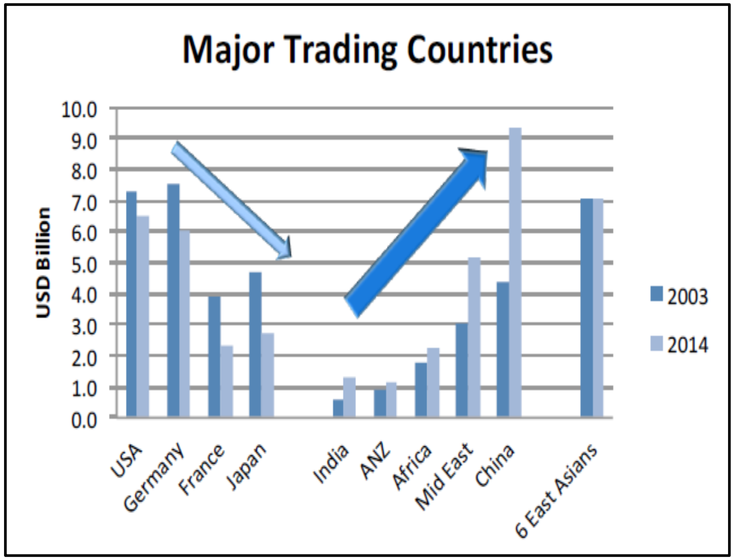
"TBML and terrorist financing (TBML/FT) refer to the process of <u>disguising</u> <u>the proceeds of crime</u> and moving value through the <u>use of trade</u> <u>transactions</u> in an attempt to legitimise their illegal origin or finance their activities.

- Trade includes both *domestic* as well as *international*

Trade Business outlook

- Global trade volumes will touch 120 trillion dollars by 2020.
- 9.62% & 9.25% CAGR in global exports & imports in 2003-2014.
- Trade is soaring at nearly double the growth rate of global GDP.
- Developed countries trade is showing declining trend and Developing countries are picking up on trade.
- Out of USD 5.49 trillion trade in Asia, 56% was within Asia.



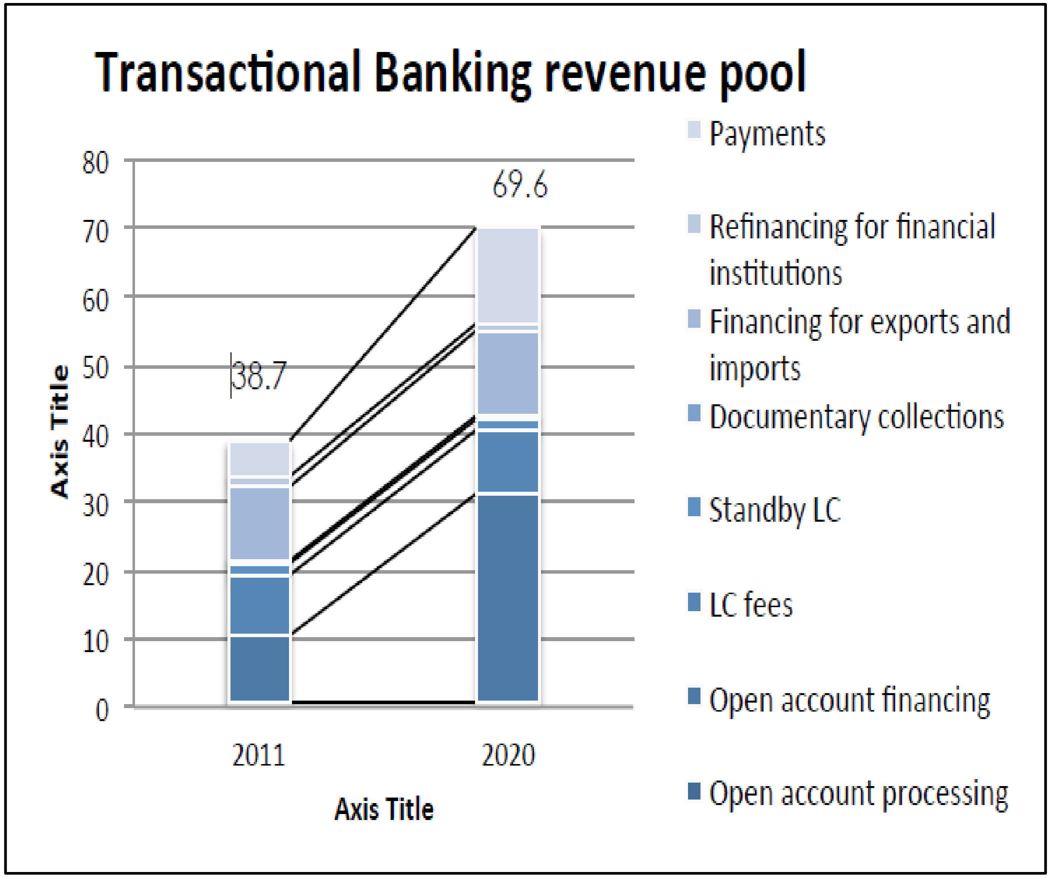


*Source – WTO data & BCG reports

Trade Business outlook

- Global Transactional banking revenues were nearly USD 1.1 trillion in 2014 and expected to reach USD 2 trillion by 2024.

- Trade related revenues likely to rise 80% in the period 2011-2020



*Source – WTO data & BCG reports

Why TBML issues arise?

- Capital controls in developing countries. It is not easy for common persons to take foreign exchange for eligible purposes easily. Trade is linked with forex markets / availability.
- Trade finance not considered as High Risk industry (except drugs or weapons)
- Cross border in nature with multiple stakeholders like manufacturer, trader, consigner, consignee, notifying party, financier shipper, insurer and freight forwarder etc.
- Lackadaisical process in trade sector. No cross-referencing of trade-data. Manual Customs data. Different Customs regimes (e.g. Free Trade Zones)
- Government Incentives for certain sector. High rate of customs duties/ Income tax.
- Different AML standards & practices in various countries. Presence of favorable structures like Hawala / Black market peso exchange.
- The high volume, regularity and speed of international Trade

TBML v/s Account based ML

TBML	Account based ML
Primary objective to move money cross border	Primary objective to integrate funds into domestic economy
Offshoot of high custom's duty/ strict foreign exchange regime	Mainly to avoid direct taxes such as income tax
Both documentary as well as non-documentary methods	Always non-documentary
Minimum use of cash	Always starts with 'placement' of cash
Channel used is cross border remittances	Domestic wires/ cheques/ digital payments

TBML methods

- Over/under invoicing’ of goods.
- Multiple invoicing of goods.
- ‘Over/Under shipments’ of goods and falsely described goods.
- Combinations of several simple techniques to make a complex structure.
- ‘Phantom shipping’ where documentation is falsified and no shipment of goods take place.

TBML Vulnerabilities

- Trade products vulnerable to
  - Advance remittances
  - Direct payments
  - Collection documents

- Sectors vulnerable to TBML
  - Diamonds/ Gems/ Jewellery
  - Multi-commodity traders
  - Software

TBML typologies – Advance remittances (1/6)

- Wash sales or round trip sales - Accounts debited and then immediately credited or vice versa for related purchase/sale
- Client is involved in high risk or cash intensive business such as money remitting
- Use of multiple accounts by customer; or accounts operated for very short period and used for advance remittances only
- Little or no withdrawal from account for business purposes/ no recurrent business expenses
- A customer deviates significantly from its historical pattern of trade activity (i.e. in terms of markets, value, freq. of transactions, volume, or merchandise type)
- Accounts funded by negotiable instruments (such as travellers' cheques, cashier's cheques, etc.) in round denominations
- Wire transfer accounts opened and closed within a very short period of time

*Source – FIU India

TBML typologies – Account based (2/6)

- Funds received but goods not exported
- Advance for exports Funds sent out but good not imported
- Advance for imports Advance for supply of goods is a major part/ percentage of the total value of goods
- Amount of advance is not in line with normal international trade for the kind of goods
- Goods not supplied within reasonable timeframe

*Source – FIU India

TBML typologies – Consignment/ Counterparties(3/6)

- Consignment size is unreasonable compared to customer profile/capacity/size of business
- Underlying goods involved in the trade transaction are of sensitive nature trade of similar items by a group of firms from the same overseas supplier (many to one) or vice-versa
- High proportion of high seas sales/merchanting trades
- Packing inconsistent with the commodity or shipping method
- Importer of goods not from the same country from where wire (payment for import) originated
- Payments/fund transfers made through economic/exchange centers even when account is held with financial institutions
- Transactions involving third parties which may not be contract parties (consignee and remitter are different)

*Source – FIU India

TBML typologies – Documentation(4/6)

- Description of goods provided is vague
- Prima facie the documents submitted look forged /suspicious
- Substantial inconsistencies between the information originally supplied and that contained in the documents
- Over/under/multiple invoicing, apparently suspect (apparently fraudulent/fake) documents
- Export/import documents are not submitted and account behaviour of the customer appears to be suspicious
- Import payments being made against old bills after lapse of considerable period of time from import of goods, without appropriate justification and documentation
- The LC contains non-standard clauses or phrases or has unusual characteristics

*Source – FIU India

TBML typologies – Location/ Valuation (5/6)

- Remittances to or from high risk jurisdictions
- Circuitous route of shipment/shipment of goods inconsistent with normal geographic trade
- Trade activity done from port which is far from the importer/exporter's base location. Example importer is in Mumbai and goods imported through a remote port in Bengal.
- Value and/or total quantity of goods is not easily ascertainable
- Significant discrepancies appear between the value of goods or services reported on the invoice and fair market value

*Source – FIU India

TBML typologies – Payment (6/6)

- Originator's bank uses <u>cover payment</u> when wiring funds to beneficiary's bank
- Structuring of transactions to <u>avoid threshold reporting</u>
- Structuring of transactions to <u>avoid submission of BOE</u> (Remittance amounts kept just below the threshold of USD 100,000 or equivalent value)
- Customer selling items on a commercial website and <u>receiving money via internet payment service provider</u>
- Originator/beneficiary information missing in wire transfers
- Use of <u>repeatedly amended or frequently extended letters of credit</u> without reasonable justification or for reasons like changes of beneficiary or location
- Frequent change in payment instruction at the last minute

*Source – FIU India

Steps to mitigate TBML risk

- Defining the ‘**customer acceptance**’ norms for offering trade products such as vintage, industry, etc
- Focusing on ‘**High Risk**’ businesses (exchange houses, travel agencies, import/export or shipping companies, grocery stores, gold and jewellery shops, textile or apparel shops, diamond dealers)
- **Branch level controls** for enhanced due diligence at transactional level
- **Monitoring of reports** submitted for trade
- Analyzing the **outstanding submission of trade documents**
- **Public domain checks, IMB checks** for trade shipments

Key challenges faced by Banks

- Lack of a central database for referencing trade transactions
- Lack of co-operation from customers
- Limited expertise available at trade operations
- Stitching up different streams of data for analysis such as account information, trade documents, customer due diligence
- Challenging to determine the fair price of the commodity
- Maintaining a balance between genuine trade v/s TBML transactions

Future initiatives

- Making custom's data available to banks
- Regulatory databases like EDPMS/ IDPMS to warn the banking participants about unscrupulous elements
- Digitization of trade documents like the demat account

Thank You

The views expressed in this presentation are that of the speaker in his individual capacity and do not necessarily reflect that of the employer

Anti Money Laundering Risk Assessment –
Challenges & Best Practices

Debmalya Maitra
Advisory Board Member
(Risk, Control, Governance & Compliance)
Fintelekt

- Background
- Framework required
- Measures to combat money laundering
- Common Challenges faced
- Case Studies

AML Framework

An AML framework consists of two major components:

1) Legal & Regulatory Initiatives

2) Institutional initiatives

<u>Legal & Regulatory Initiatives</u>

•Minimum standards as laid down by FATF

•Country and Regional Risk perception

•Industry specific programmes and Reporting requirements

AML Framework (cont.)

<u>Institutional Initiatives</u>

- Industry & Business specific risk assessment
- Creating awareness within the organisation
- Setting up of the reporting structure
- Maintenance of key records

Some major regulatory actions

- In 2012, HSBC Holdings, a London-based company, paid nearly $2 billion in fines after it was discovered that they laundered money for drug traffickers and other organized crime groups throughout Iran. The laundering went on for many years before being detected

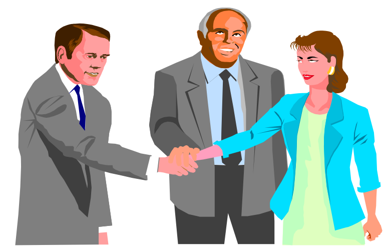
- In 2014, BNP Paribas, a French bank headquartered in London, pled guilty to falsifying business records after it was discovered they violated U.S. sanctions against Cuba, Sudan and Iran. BNP paid a fine of $8.9 billion which is the largest such fine imposed

- In the 1980s, the Bank of Credit & Commerce International, registered in Luxembourg and with offices in London, was found guilty of laundering amounts estimated to be in the billions for drug traffickers

Measures to combat Money Laundering

AML training
(mandatory for all employees, outsourced partners & Agents)

Know Your Customer



Close cooperation with Regulators, FIU, Law enforcement agencies, Interpol, etc

Monitoring and Surveillance

Common Challenges faced

Management Structure

<u>Concern</u> - The management structure to ensure AML compliance is not well defined

<u>Best Practices</u>

- ‘Tone at the top’ should be clear
- Responsibilities of the top management and the Board should be clearly defined
- The Money Laundering Reporting Officer (MLRO) should be a sufficiently senior person with access to all records and information necessary for discharging his duty

Policies and Procedures

<u>Concern</u> – Policies & procedures are not updated in light of current environment

Best Practices -

- Any major change in the regulation should be updated at the earliest, with at least an annual review of the policy by the Board of Directors
- The policy should in addition to covering legislative & regulatory requirements, also reflect risks involved with the industry, institution and the kind of products offered by them
- Any change in operating process should be evaluated to identify the risks involved
- The AML risk should be evaluated at the time of launch or withdrawal of any product so that processes can be updated immediately

Know Your Customer (KYC)

<u>Concern</u> – The KYC programme is diluted in practice by :

- **providing facility larger than that is justified by the financial statements**
- **Not co-relating transactions to nature & volume of business declared by the customer**
- **Not updating the current KYC details of the customer**

Best Practices -

- The KYC programme should be regularly tested and weaknesses should be strengthened
- Every institution should update the KYC framework based on changes in business mix
- The KYC records should be regularly refreshed, to ensure that rules are able to identify negative trends
- The definition & identification of Politically Exposed Persons (PEPs) should be clear and properly recorded in all cases

KYC – Enhanced Due Diligence

- A risk based KYC framework should be developed, wherein basic checks and enhanced due diligence checks are clearly defined by a rule based framework

Enhanced due diligence should be :

- commensurate with the level of risk perceived based on customer's business, financial & transaction profile. A risk classification of the customer into High, Medium or Low should be done
- augmented by inputs from UN /OFAC/ EU suspicious list
- Local intelligence should be regularly gathered and should draw not only on records and information supplied by the customer, but also any public information from news agencies and other sources

Know your employee (KYE)

<u>Concern</u> – The number of compliance violations involving employees is showing an increasing trend

Best Practices -

- Stronger pre-recruitment background checks of employees should be conducted, including front line employees who are at the start of the value chain
- Credit worthiness, education and employment checks should be the minimum level of check. Psychometric testing is an added check point
- Checks should also be conducted on role change or increase in grade of employee
- High attrition in sensitive positions should also be closely monitored

Record Maintenance

Concern – Record Maintenance Policy is not drawn up in a smart manner to facilitate record recovery

Best Practices -

- All institutions should have a clear record maintenance policy, based on the local and international laws and regulations
- In case a particular transaction or account is reported as suspicious transaction, records for the account should be maintained for a minimum period of say 5 years after the account is closed
- The record maintained should be in line with the legal framework i.e. Evidence Act – if permitted, the records can be maintained in digital form also

Interaction with Regulators & FIU

Concern – The FIU, industry regulators and institutions are not on same page on the various issues

Best Practices -

- There should be regular meetings between above stakeholders, to ensure guidelines are uniformly understood & implemented
- The effectiveness & adequacy of reports submitted should be reviewed from time to time and feedback provided to the respective institutions
- Feedback from the authorities should be discussed internally and form a basis for changes in processes

Generation of Alerts and Reporting

<u>Concern</u> – Too many alerts generated leading to frivolous reporting or too few resulting in inadequate reporting

Best Practices -

- Reporting parameters should be carefully defined to ensure alerts are neither numerous or irrelevant
- In some places, the industry association, regulator & FIU agree on broad parameters of an alert
- Verification of alerts should be done independently by the AML team, though explanation should be sought from the relevant business unit
- The decision on reporting of a transaction or account as suspicious should ultimately rest with the MLRO
- The number of suspicious transaction reports should be commensurate with the size and nature of the organisation

Training

Concern - The training process becomes ineffective

Best Practices -

- AML guidelines must be understood well by frontline and operating staff covering:
    - At the time of induction
    - Regular refresher training
    - Periodic awareness programme for the top management and the Board of Directors
- It is important to keep the training material up to date and create a bank of assessment questions and case studies which are not identical. This ensures that the matter does not become mundane or predictable
- A proper system to record the training and assessment should be maintained, to ensure that the guidelines are complied to, in both letter and spirit
- An MIS to the management should be provided regularly to measure the effectiveness of the programme

Risk Assessment – Areas of safeguard

- Customisation of the risk assessment rules to ensure that false positive cases are in control
- Assessment the product and customer risk profile on an ongoing basis
  - Change in customer profile is assessed at regular intervals
  - Updates from customers are properly documented
  - Changes in certain external condition leading to change in risk profile of a product
- Ensure action on alerts are based on well documented logic
- Proper updating of caution list based on local intelligence

Case Study I

Cobrapost Sting operations

A journalist of a digital magazine 'Cobrapost' posing as a relative of a fictitious politician offered to deposit/ investment large sums in cash without adequate details.

This sting revealed that none of the banks & insurance companies that were approached turned him down and instead offered him solutions to launder the money. A total of 23 public and private financial institutions were implicated in this sting operation.

In one case, a bank stated that they would only question the investor about the source of money, when such investment in insurance policies exceeded Rs. 1 crore

Case Study II

Benami (Anonymous) Transactions

A retired government engineer put substantial money in insurance policies (regular premium) and later on claimed that the policies have been mis-sold to him with a promise of bonus payment against his earlier policies.

Considering his age and some signature mismatch, the amounts were refunded.

He then came back and registered his email id against two other customers who had also bought regular premium policies with substantial premium.

•Both these persons had claimed to be Agriculturists

•In India agricultural products is exempt from income tax, so they do not have Standard Income proof.

•In one case a Fixed Deposit receipt was deposited to demonstrate the financial capacity of the customer

Later the original customers refused to come forward and this person started corresponding with the company claiming:

•funds belong to him

•it was invested because of promises made about returns / bonuses

•FD receipt submitted was fake.

•Refund should be made on that basis well after the freelook period

AML and Enterprise Risk Management

- It is important to treat AML as a risk management tool and make it a part of the overall risk management project, as these will assist in managing risks such as :
  - Fraud Risks
  - Credit Risks
  - Process Risk
  - People Risks

Questions ???

Thank You

AML/CFT: Changing Dimension

Hari Kumar Nepal
Deputy Director/NRB
Advocate/Certified Anti-Money Laundering Specialist (CAMS)
Ph.D. Research Scholar on AML/CFT

Objectives of the Program

- Recognizing the change in policy dimension
- Pursuing cozy implementation modalities

Ultimate Objective

- **Financial systems and the broader economy are protected** from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.

Changing schools

- Business vs. AML or AML for Business
- Financial inclusion vs. exclusion
- Strengthened CDD & less-painful/useful updates
- Risk based approach
- Explored beneficial ownership
- Intensified monitoring and qualified SAR/STR
- System/institution protected from abuse
- Effective & result oriented implementation
- Outcome not only output
- Self assessment & coming up Mutual Evaluation
- Non-tolerance of non-compliance with stringent actions

Functional Frameworks

- Executing AML/CFT Policy & Compliance Program
- Understanding CDD/KYC or KYCC Mechanisms as it is (Complex, multilayered, unending job with
    - Identification/verification (Risk based, PEP)
    - Objective/Purpose
    - RBA
    - Beneficial ownership & controls
    - Terrorist , PEP & other negative list check
    - Enhanced CDD
    - Less painful and useful updates
    - Informal information collection
    - Anonymous A/C or system vulnerability

Functional Frameworks (Contd...)

- Risk based approach
    - National Surrounding
    - Institutional environment
    - Customer
    - Geography
    - Product/Services
    - Transactions
    - Delivery Channel
- Monitoring & Detecting STR & Reporting
    - No standing mechanisms
    - Nominal STRs
    - Misuse of the products & system : Corporate vs. individual A/C, house wife, student, growing corporate vehicles
    - **Terrifying tax evasion followed by corruption (UNODC Report ?)**
- Internal Controls/Managements/Capacity Building: System, Budget, Programs)
- Record Keeping

Mutual Evaluation:
Outcomes rather than output

Technical Evaluation (40)

Risk and Context

Conclusions

Recommendations

Effectiveness Evaluation (11)

Assessment Ratings

High-Level Objective:

Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.

Compliance/Achievement Ratings	
Technical	**Effectiveness**
Compliant	High level of effectiveness
Largely compliant	Substantial level of effectiveness
Partially compliant	Moderate level of effectiveness
Non-Compliant	Low level of effectiveness

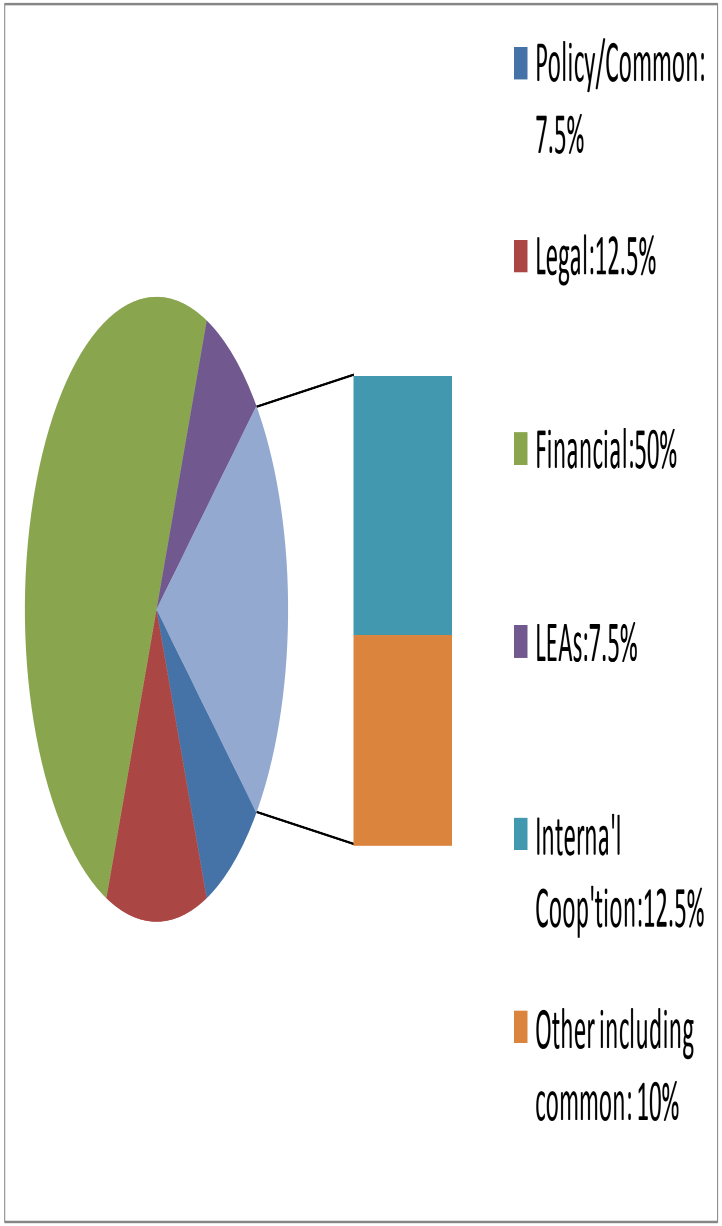
Criteria for Enhanced Follow up

- Previous : 10 or more NC/PC on Core or Key

Current:

- 8 or more NC/PC on technical compliance, or
- 1 or more NC/PC on following; or
  - 3 - Criminalization of ML, 5 - Criminalization of TF, 10 - Customer Due Diligence, 11 - Recording Keeping of BFI & Others, 20 – Reporting of STR
- 7 or more of 11 effectiveness outcomes rated low or moderate level, or
- 5 or more of the 11 effectiveness outcomes rated low level.

Financial Sector : holds more than 20 fundamental Recommendations or more than 50 % of the system;
75 % laundering and TF through Financial Sectors



Way Forward

- **Robust and ruthless implementation of AML laws**
- **Robust systematization and fuctionalization**
- **Avoidance of future risks (Not being vehicle & victim)** :
  - Individual/Institutional/National/International
  - Abuse of products/institution & system
  - Shift from doing to done
- **Capacity building :**
  - **Knowledge/skill test /Automated system**
  - **OUTCOME NOT ONLY OUTPUT**
- Zero tolerance also with eyes on 2019/020 assessment

- AML/CFT is a hen laying golden egg for the country; &
- for **Protecting us, Our financial system, Our country and the world.**

It's a beginning ...