

INTRODUCTION TO CONCURRENT AUDIT

KYC & AML COMPLIANCES

Concurrent Audit

- Part of a bank's early warning system to ensure timely detection of irregularities & lapses to prevent fraud.
- Attempts to shorten the interval between a transaction & its examination by an independent person
- Checking is contemporaneous or immediately post the transaction is completed.
- Emphasis on substantive or in depth checking
- Management process integral to a sound internal controls

Scope & Objectives

- Supplements bank's efforts in carrying out simultaneous internal check of the transactions & other verifications & compliance as per laid down procedures.
- Scope focused to cover fraud prone areas like
 - Handling of cash
 - Deposits
 - Advances
 - Foreign exchange business
 - Off-balance sheet items
 - Credit-card business
 - Internet banking

Identification of high risk areas & improve branch functioning leading to risk mitigation & fraud.

Principles

- Ensure observations are seriously attended & closed to improve overall branch functioning.
- Hold monthly meetings to create “awareness”
- Adopt constructive, corrective & practical approach.
- Adopt helpful & positive attitude & not be guided by impulsive or hostile attitude.
- Good understanding of job profile, analytical capacity & sound knowledge of existing banking procedures & practices.
- Sufficient knowledge & skill to work in CBS / computerized environment.

Accountability

- Responsible for material omission or commission in respect of transactions.
- As per RBI guidelines, accountability is failure to comment on –
 - Fraud
 - KYC adherence
 - Income leakage
 - Frequent recurrence of deficiencies in successive audits
 - Any other serious irregularities
- Which could have been ascertained by exercise of due diligence.
- In a serious case of omission or commission in working of audit, bank can consider termination & report to RBI & ICAI.

Areas to be Covered

- Cash
- Investments
- Deposits
- Advances
- FX Transactions
- Housekeeping
- Other Items
 - Audit Compliance
 - Customer Complaints
 - Verification of HO & Statutory returns

Items Eligible for 100% Checking

- Off-Balance Sheet Items (LC & BG)
- Investment Portfolio
- Foreign Exchange Transactions
- Fraud prone/sensitive areas
- Advances with outstanding balance $>$ Rs.500000

Checkpoints - Advances

- Loans disbursed before the compliance of pre-sanction conditions.
- Follow-up of post disbursement sanction terms.
- Mechanism for monitoring of weak accounts.
- Advances to defaulters in other banks.
- Ratification/ approval of higher authorities wherever necessary.
- Justification of repayment capacity of borrower.
- Tracking of penal interest – manual or automated.
- Timely submission of financial statements where required.
- Mechanism for monitoring fund diversion.

Checkpoints - Housekeeping

- Debits to income heads
- Transactions in staff accounts
- Detection & prevention of revenue leakage
- Reconciliation of ledgers
- No. of cheques bounced & cases under Section 138 of NI Act

FX

- 100% checking of Bills of Entry
- Monitoring debits & credits in FCNR & NRO A/c's.
- Remittance forms (A-1,A-2)

Checkpoints – Other Areas

- Correctness of data entry in CBS
- Exceptional Transaction Reports
- ATM Complaints & redressal
- Written declaration of beneficiary or remitter for large RTGS amounts
- Availability of adequate copies of BCSBI code & other information manuals at the branch.
- Information security & BCP

Need for Paradigm Shift

- Shift from transactional audit to risk based audit
- Purpose of concurrent audits is to find gaps in processes & suggest solutions.
- In depth study of procedures.
- Take measures to prevent gaps between queries raised by concurrent auditors & RBI/statutory/internal auditors
- Do not base conclusions on INQUIRY.
- Data – Information – Knowledge - Wisdom
- Hindsight – Insight – Foresight

‘Best practices are always a moving target’

Know Your Customer (KYC)

- Most underrated area in a concurrent audit is compliance of KYC & AML norms.
- Is this area emphasized on with the same rigor as credit monitoring? Are we considering Money Laundering Risk ?
- Is there a mechanism in place which monitors accounts requiring enhanced due diligence?

KYC means -

Making reasonable efforts to determine –

- True identity & beneficial ownership of accounts;
- Sources of funds
- Nature of customers' business
- Reasonable account activity
- Customer's customer




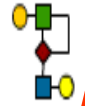
Customer

- Who maintains an account,
- Establishes business relationship,
- On whose behalf account is maintained
- Beneficiary of accounts maintained by intermediaries,
- Who carries potential risk through one-off transaction

What you should know?

- True identity & beneficial ownership of accounts
- Permanent, Registered & Administrative address

Core KYC Elements

	<p>Customer Acceptance - Ensure that only legitimate & bona fide customers are accepted.</p>
	<p>Customer Identification- Ensure that customers are properly identified to understand the risks they may pose.</p>
	<p>Transactions Monitoring- Monitor customers accounts & transactions to prevent or detect illegal activities.</p>
	<p>Risk Management- Implement processes to effectively manage the risks posed by customers trying to misuse facilities.</p>

Guidelines issued by RBI, SEBI & IRDA

Risk Rating Methodologies

At the account opening level classify customer based on the RISK attached to him into following 3 ratings keeping in mind the profile of the customer being rated

Low Risk

- well defined salary structure
- Businessman / Traders with well defined activities & transactions commensurate with business
- Low balances / Turnover in accounts

Medium Risk

- NBFC, brokers, Travel agents, Tele-marketers
- Sole practitioners, Advocates (small- little known)
- Importers/ Exporters etc.
- Cash intensive business e.g. Retail stores, Restaurants, 2nd hand car dealerships etc.
- Dot-com companies
- Venture Capital Companies

High Risk Customers

- NRIs, HNIs, PEP
- Property dealers / builders
- Co's with close family shareholding
- NPOs
- Firms with sleeping partners
- Non face to face customers
- Embassies/ Consulates
- Client A/cs managed by professional service providers Eg. law firms, accountants, agents, brokers, fund managers, trustees, custodians

Risk Rating Review-

- As per **RBI guidelines** review of risk categorisation of customers should be carried out at least once in **6 months**.
- It will ascertain customers who need enhanced due diligence
- **An ideal system-**
 - Updating parameters for review in the current AML system
 - Exploit the existing thresholds.
 - Movement in Risk Rating of A/c's as we do NPA's

Parameters for Review

Business Intelligence

- Customer Constitution
- Business Segment/Occupation
- Country of residence/nationality
- Product subscription
- Account status

Transaction Type

- Cash
- Clearing
- Transfers/Remittances

Transaction Trend

AML Alerts/ Signals

Periodical Updation of KYC

- Continue carrying on-going due diligence
- Closely examine the transactions to ensure
 - Consistency with client knowledge,
 - Nature of business
 - Risk profile
 - Source of funds
- Full KYC exercise will be required to be done every:
 - 2 years for high risk accounts
 - 8 years for medium risk
 - 10 years for low risk

Accounts NOT to be opened by Banks

Benami or anonymous accounts

Accounts of known criminals or banned entities

Shell banks

Pooled accounts on behalf of clients by Lawyers & Accountants who are bound by customer confidentiality

Types of Customers

Non Face to Face Customers

- Apply Enhanced procedures to mitigate the higher risk
- First payment to be effected through the customer's account with another bank
- Presents a greater money laundering or terrorist financing risk - inherently difficult to ascertain the identity of the person.

Accounts of Politically Exposed Persons (PEPs)

- Gather sufficient information available in public domain.
- Seek information about sources of funds.
- Decision to open the A/c to be taken at senior level & mentioned in the form
- A/c subject to enhanced monitoring
- Same process to be applied to family members of PEPs

Financial Corridors

- Remittances to high risk jurisdictions are sent through other countries.
- Transactions should be **treated** in the same way as **high risk jurisdiction**
- For eg:- Yemen may be sent through UAE before being finally sent to Yemen.

Beneficial Owner(BO)

- Person behind the customer-owns/ controls the customer
- On whose behalf a transaction is carried out
- Be alert while analyzing the transactions in accounts by identifying the Beneficial owner
- Understand the true nature of the A/c's maintained by the intermediary
- Eg: Tailor/Maid/ Servant depositing cash or cheques of high amount, huge turnover in a minor's account etc

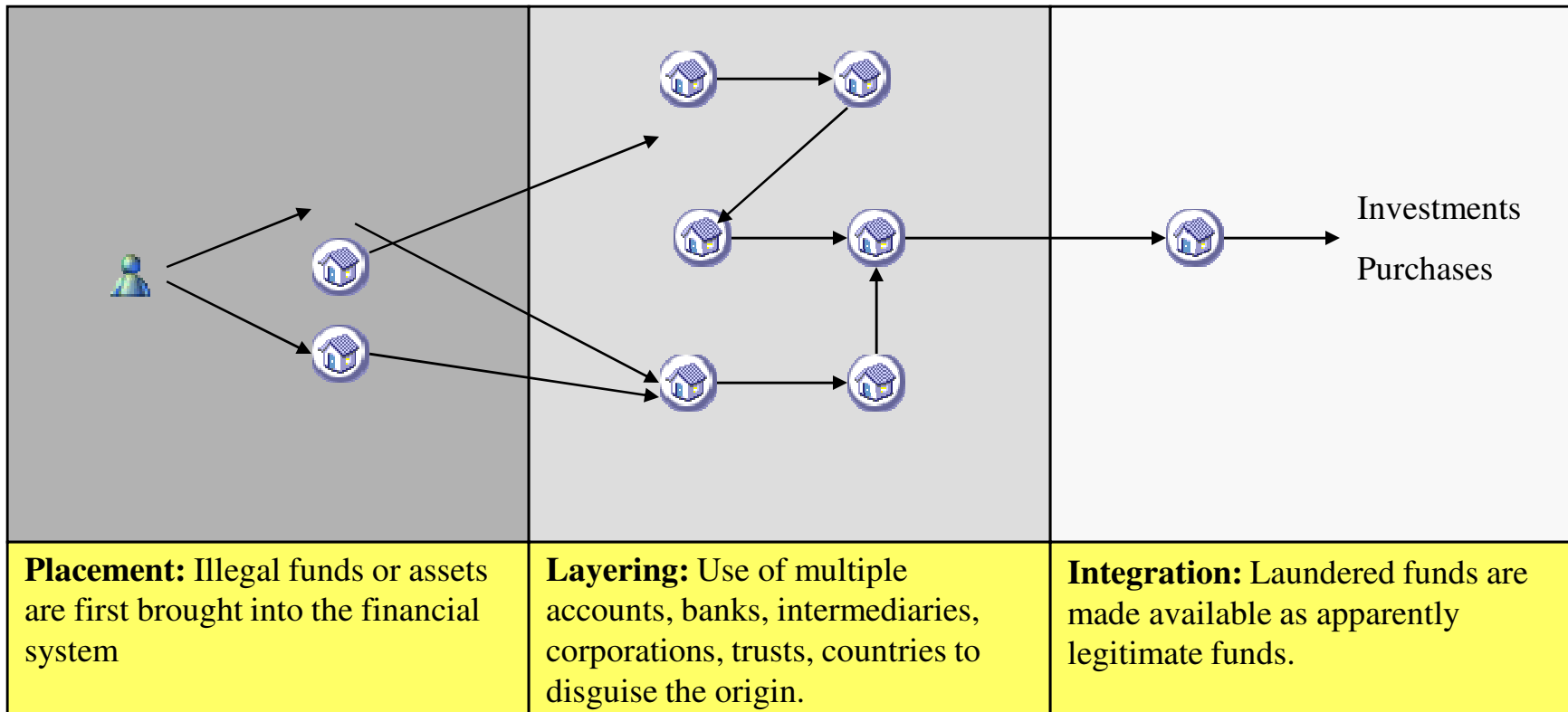
Gaps in KYC

- The problem is not with KYC, but its implementation.
- Industry Regulator- Improve frequency & quality of inspection
- Government- Need to speed up Aadhar to eliminate multiplicity of documents
- Banks- Aggressive sales culture

What is Money Laundering ?



Money Laundering is the process by which illegal funds & assets are converted into legitimate funds & assets.



Important: All money laundering transactions need not go through this three-stage process.

Money Laundering Risks

All risks are inter-related & together can potentially cause serious threat to the survival of the bank

- Reputational risk
- Legal risk
- Operational risk (failed internal processes, people & systems & technology)
- Concentration risk (either side of balance sheet)

‘Is this risk considered for a customer with the same rigor as a credit risk is considered for a borrower?’

Legislative & Regulatory Framework

- Prevention of Money Laundering Act, 2002 (PMLA, 2002)
- Recent Amendments in Prevention of Money Laundering Act (PMLA) & PML (Maintenance of Records) Rules
- Unlawful Activities (Prevention) Act, 1967
- Financial Action Task Force (FATF)
- Reserve Bank of India (RBI)
- Financial Intelligence Unit – India (FIU-IND)
- Indian Banks Association (IBA)

Reporting Requirements

- **Prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities**

In terms of the **Rule 3 of the PML** (Maintenance of Records) Rules, 2005, Banks are required to furnish following to the Director, FIU-IND


- Cash Transaction Report (CTR)
- Counterfeit Currency Report (CCR)
- Suspicious Transactions Report (STR)
- Not for Profit Organization Transaction Report (NTO)
- Cross Border Wire Transfer (CBWT/EFT)

Report	Periodicity	Description
CTR	15 th day of succeeding month	<ul style="list-style-type: none"> a) Cash transactions above Rs. 10 lakhs or its equivalent in foreign currency b) Cash transactions integrally connected to each other below Rs. 10 lakhs or its equivalent in foreign currency in a month
CCR	15 th day of succeeding month	<ul style="list-style-type: none"> a) Cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine b) Forgery of a valuable security or a document has taken place facilitating transactions
NTR	15 th day of succeeding month	Receipts by NPOs of more than Rs. 10 lakhs or its equivalent in foreign currency
STR	Within 7 working days on the transaction being determined suspicious	<ul style="list-style-type: none"> a) Based on 54 Red Flags issued by IBA b) Based on Law Enforcement Queries received by Bank c) Based on Media Reports & Public Complaints d) Monitoring by employees
CBWT	15 th day of succeeding month	All cross border wire transfers of more than Rs. 5 lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India

SUSPICIOUS TRANSACTION

Transaction whether or not made in cash which, to a person acting in good faith –

Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime



Appears to be made in circumstances of unusual or unjustified complexity



appears to have no economic rationale or bonafide purpose

Grounds for Suspicion

- **Activity in accounts**
 - Unusual activity compared with past transactions
 - Sudden activity in dormant accounts
 - Activity inconsistent with what would be expected from declared business
- **Identity of client**
 - False documents
 - Identification documents which could not be verified within reasonable time
 - Accounts opened with names very close to other established business entities
- **Background of client**
 - Suspicious or links with known criminals
- **Multiple accounts**
 - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
 - Unexplained transfers between multiple accounts with no rationale
- **Nature & value of transactions**

Alerts for Identifying Suspicious Transaction

- Alerts through AML Package
- Behavioral Alerts
- Notice/Letter from Law Enforcement Agency
- Adverse Media News
- 54 Red Flag Indicators by IBA
- CTRs & NTRs
- Monitoring Accounts of Multi Level Marketing Firms
- Beneficial Owner
- Trade Finance
- Overseas Forex Trading through Electronic /Internet Trading Portals
- Demat A/cs
- Locker Transactions

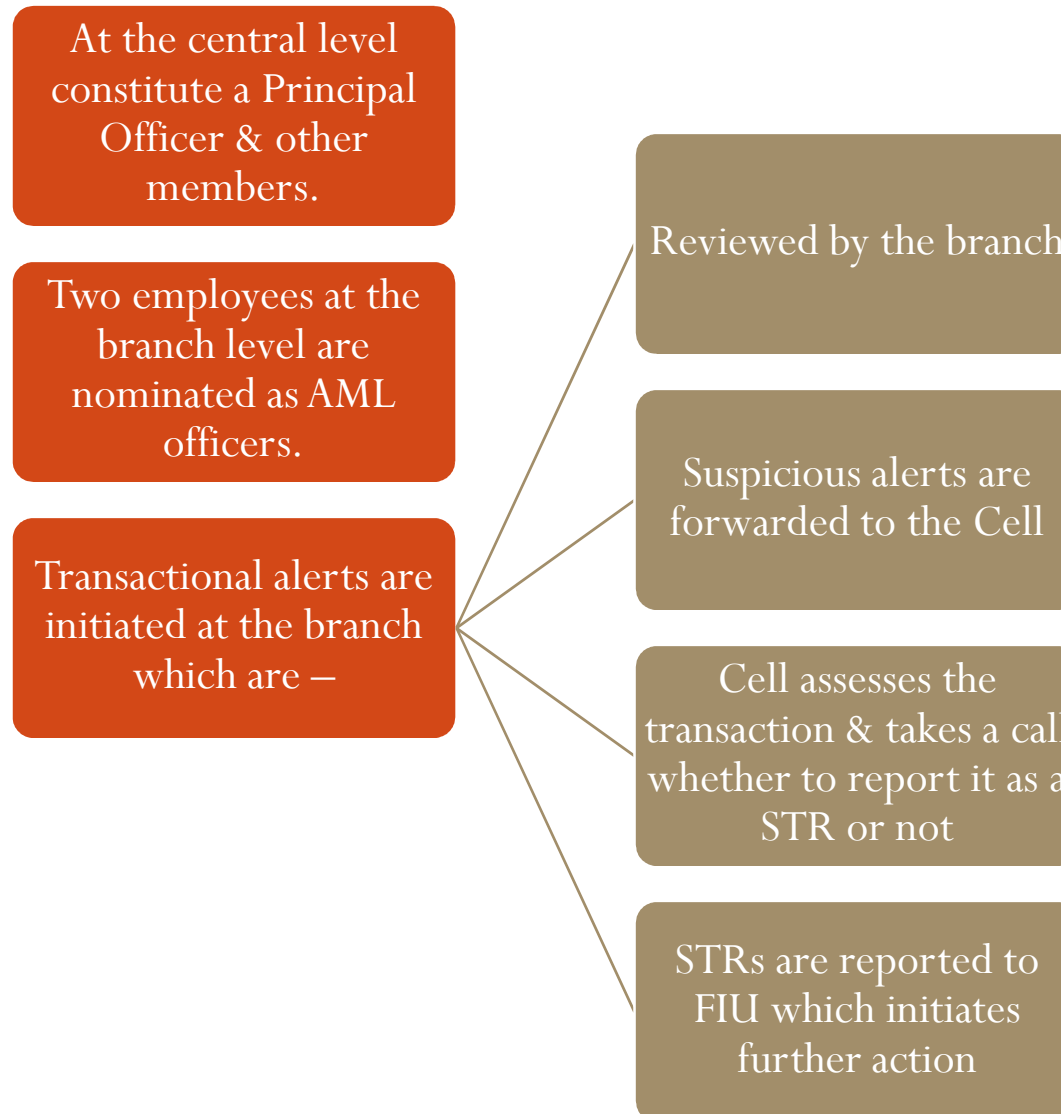
IBA Customer Behavioral Indicators

- Reluctancy to provide information
- Unusual curiosity
- Giving confusing details
- Refuse to give reason for a transaction
- Numerous deposits & withdrawals
- Avoiding contact with branch
- Unexpected repayment of loan
- Account with multiple institutions

54 Red Flags by IBA

- The AML software is programmed to generate alerts based on thresholds which relate to the 54 Flags
- Red Flags can be broadly divided into four categories:
 - **Watch List (WL)**: The customer details matched with watch lists - UN list, Interpol list etc.
 - **Typology (TY)**: Common typologies of money laundering, financing of terrorism or other crimes - structuring of cash deposits etc.
 - **Transaction Monitoring (TM)**: Transaction monitoring alert - unusually large transaction, increase in transaction volume etc.
 - **Risk Management System (RM)**: Risk management system based alert - high risk customer, country, location, source of funds, transaction type etc.

Working of a Decentralized AML Cell



Money Mules

- Used to launder the proceeds of fraud schemes (e.g. phishing & identity theft) by criminals who gain illegal access to deposit accounts by recruiting 3rd parties to act as “money mules.”
- 3rd parties may be innocent or have complicity with the criminals.
- Recruited by a variety of methods, Eg: spam e-mails, advts on genuine recruitment web sites, social networking sites, instant messaging & advts in newspapers.

An individual is recruited to receive cheque deposits/wire transfers



Transfer these funds to A/cs held on behalf of another person or to other individuals,



For a certain commission payment

Gaps in the system

- AML software throws numerous transactional alerts.
- For monitoring non-automated parameters-
 - Training to be imparted to staff at the branch level
- Documentation of reasons for classifying a transaction as normal & not reporting is as STR
- Maintenance of audit trail to be in place for auditors to assess whether the process laid down on paper is being followed

Gaps in KYC - AML

- Poor quality of data - false positives & less time to focus on the real risks
- Data scale is massive & diverse -Single view of client transaction missing
- Understaffed & Untrained Human Resources & lack of incentives to blow the whistle on black money
- Lack of support from strong processes & technology – use of data analytics
- Check Box approach
- Revenue generation pressure forcing dilution of norms
- Profit maximization drives banks beyond core tasks, to hawk products such as equities, insurance & mutual funds.
- No verification of customer's address or job. Risk assessment mostly re-actionary
- Absence of robust & ongoing due diligence process – especially risk profiling
- Processes not implemented strongly during modifications
- Security around creation/ modification of client – account master not strong enough.
- Communication gaps between Marketing – Sales & Risk / Compliance – Centralized decentralized operations

Identification & Assessment of Risk

- **Adoption of a Risk Based Approach in implementing**
 - customer acceptance policy,
 - customer identification procedures,
 - transaction monitoring &
 - risk management
- Customer Risk
- Product & Service Risk
- Geographic Risk

Responsibilities of Banks

- By law, bank employees have authority to ask a customer for details of transactions not consistent with customer's profile.
- Onus is on the bank to ensure that the account is not being used to launder money.

Former RBI governor Bimal Jalan says:

"We should learn from the current experience & see how we can improve our ethical governance system in implementing the banking guidelines."

Measures to Deter Money Laundering

- Zero tolerance for KYC – AML breaches
- Tone at The Top – Walk the Talk -
- Consider ML risks in daily operations, develop new financial products, establish new business relationships & changes in customer profiling.
- Screening of employees before hiring & those accessing sensitive information
- Appropriate quality training to staff
- Quick & timely reporting of suspicious transactions
- Complaint resolution / Whistle Blower system

Banking Frauds

- **Deloitte Indian banking fraud survey Edition II April 2015** states - frauds in the Banking sector have increased by more than 10% in the last 2 years.
- The average fraud loss was 2 lakhs in the retail segment & 2 crores in the non retail segment.
- In majority of the cases recovery of fraud was less than 25% of the fraud value
- Concurrent audit system prevalent in banks as a part of the recommendations of the Ghosh committee was a direct fallout of the Harshad Mehta scam- It was set up to serve as an early warning signal to prevent serious irregularities & frauds.

Banking Frauds

The root cause of all Banking Frauds - failure to know 3 vital entities that it deals with in the banking business.

To prevent Fraud 3 KYs to be considered:

- **Know Your Customer**
 - **Know Your Partner**
 - **Know Your Employee**
-
- The top 3 fraud risks that are the highest concern for banks are –
 - Internet banking
 - ATM fraud E banking (Debit & Credit card)
 - Identity fraud.

‘If you see fraud & do not say fraud, you are a fraud’

Nassim Nicholas Taleb

Frauds Listed By RBI

As per yearly master circular issued on 1st July –

- Mis-appropriation & criminal breach of trust
- Fraudulent encashment through forged instruments, manipulation of books of accounts or through fictitious accounts & conversion of property.
- Unauthorized credit facilities extended for illegal gratification or reward
- Negligence & cash shortages – over Rs 10,000/- & over Rs 5,000/- if detected by inspecting officials or auditors & not reported on the day of occurrence by the persons handling cash
- Cheating & Forgery
- Irregularities in Foreign Exchange Transactions
- Any other Fraud not coming under the above specific heads.

RBI-Frauds by Borrowers

(A) Fraudulent discounting of instruments or kite flying in clearing effects

(B) Fraudulent removal of pledged stocks / disposal of hypothecated stocks without the knowledge of the bank / inflating the value of the stocks in the stock statements & drawing excess bank finance.

(C)

- 1) Diversion of funds
- 2) Lack of interest
- 3) Criminal neglect in adhering to financial discipline
- 4) Managerial failure with mala fide intent leading to the unit becoming sick
- 5) Laxity in effective supervision over the operations rendering the advance difficult for recovery & resulting in financial loss to the bank.

Frauds typical to Banking Industry

- **Cheque frauds** – alteration / impersonation
- **Accommodation Bills** – These are drawn & accepted without any consideration passed or received.
- **Ever greening or Window Dressing of NPA accounts** – The purpose is to show lesser NPA and consequentially higher profits by reduced mandatory provisioning.
- **Auction frauds** – Low bids are accepted & the difference with the market price is shared to agreed extent.
- **Debt Restructuring frauds** – hiding or transferring asset before filing for bankruptcy by knowingly concealing or mis-stating the assets, the debtor abuses the process to escape financial liabilities
- **Rogue Traders** – engages in unauthorized trading to recoup the loss he incurred in earlier trades. Out of fear & desperation, he manipulates the internal controls to circumvent detection to buy more time.
- **ATM – Debit / Credit card frauds**
- **Bank robberies**
- **Unauthorized Operations** in dormant accounts / Pay-orders / Demand drafts –
- **Use of suspense a/c's / old reconciliation** balances to adjust unauthorized entries.

Willful Defaulters

- RBI in its Master Circular on Willful Defaulters has defined Willful Default as –
 - Defaulting in repayment obligations despite having the capacity to honor the same.
- Criminal Action will be taken against borrowers diverting funds with mala fide intent.
- Wrong certification of end use of funds will also attract criminal action against the borrowers.

Prevention of Frauds

An annual review of the frauds to consider whether-

- Systems are adequate to detect frauds
- Frauds are examined from staff angle & action taken without delay
- Deterrent punishment is meted out to the persons found guilty.
- Frauds have taken place because of laxity or loopholes in systems & procedures or loopholes in the system.
- If so, whether effective action has been taken
- Frauds are reported to the local police for investigation

Case Study 1 – Gaps in KYC/AML

What happened?

- A Bank received Rs. 110 crs from a Trust through RTGS for Fixed Deposit.
- Due to pending KYC compliances the amount was parked in Sundry Deposit a/c
- Before an FD could be created instructions were received by FAX from the trust to transfer the amount to a 3rd party XYZ International.
- Another amount of Rs.70 Cr was transferred in a similar manner.
- Meanwhile a reminder from the trust was received for the FD receipts.
- This is when the Bank realized a fraud had taken place.

What went wrong?

- The Bank appeared to be eager & too pleased to receive a big amount towards FD as new business.
- The Bank did not complete KYC formalities immediately upon receipt of Rs.110 Cr for Fixed Deposit or soon thereafter.
- It was a grave mistake on the part of the Bank to accept the instruction sent through fax.
- Since the Bank did not have any record of KYC with them, they should have refrained from allowing any transaction against purported Fixed Deposit.
- Even in the normal circumstances, instructions by FAX are accepted only after proper safeguard including undertaking, indemnity etc. by the account holder.

Case Study 2 - Gaps in AML

- An ongoing scam came to light after officials pointed out the suspicious transactions to the investigating agencies.
- Lapses at Bank's end ??
 - Banks are expected to raise exceptional transaction reports (ETRs) & suspicious transaction reports (STRs) with the RBI in case of discrepancies.
 - delay in pointing out these discrepancies resulted in the scam gaining momentum.

Case Study 3– Money Mules

- Fx transactions carried in newly-opened current accounts where heavy cash receipts observed, but no red flags raised.
Current a/c opened in names of rickshaw-pullers, street vendors, domestic helps who were made ‘directors’ in fake companies.
- These persons paid Rs.10,000 to 15000 p.m for lending their IDs.
- Black money sent to shell companies in Hong Kong through these fake companies.

Case Study 4 - Beneficiary Owners

- Transfer of thousands of crores to Hong Kong through a single branch of a Bank had benami or anonymous actors.
- XYZ from the mining town of Chibasa in Jharkhand is 'small' coal trader-**A FAKE FRONT**
- Owns a company ABCD Ltd. in Hong Kong to which millions of dollars were transferred, was controlled by a **beneficiary.**

Case Study 5 - Money Laundering

- A bank was involved in laundering money for Mexican drug cartels & moving the same to Saudi Arabian banks with ties to terrorists.
- It also flouted US law by transferring money through its American subsidiary for sanctioned nations, including Iran, Sudan & North Korea.
- **Issues:**
 - No monitoring of transactions
 - Lack of compliance officers to check suspicious transactions
 - No reporting of suspicious transactions
 - No KYC compliances
- **Penalty:**
 - It paid a penalty of \$665 million, (INR 4000 Crores) highest paid penalty ever recorded .

Case Study 6 - Fraud

- M/s X a proprietary concern opened a Current A/c.
- Business Profile- Import of cutlery items
- Turnover of Rs. 716.75 Lacs in a span of 3 months
- He had a balance of Rs.68 Lacs in the CA.
- The credit proceeds were by way of inward remittances through RTGS which were then remitted abroad to Hong Kong & China against import of goods.
- In order to verify the HTR a visit was made by branch officials at his business address & it was revealed that the office has shifted. Thereafter a visit to residential address revealed that the building was under redevelopment.
- Though he submitted fresh KYC documents, the officials verified the authenticity of Bill of Entry from ICE-GATE website where no entry was found.

Case Study 7- Identity Theft

HUF account in the name of Mr. X was opened.

- A cheque of Rs.28 Lacs was deposited drawn by ABC Hsg Finance upon clearance the entire amount was withdrawn in cash.
- Subsequently a police inquiry asking whether accounts were opened in the name of a Mr.X & Mr.Y .The police station had received a complaint from one Mr. X staying in their jurisdiction.
- On investigation it was revealed that the HUF account was opened by impersonating the name of Mr.X by submitting a fudged PAN.

What went wrong:

- Branch did not question the withdrawal in cash.
- Cash withdrawal by the party was thrown as an alert by the AML software. The branch rejected the transaction being suspicious citing the nature of business as real estate & construction.
- No proper mechanism in place to verify the authenticity of the Proofs of identity & address.

Case Study 8 - STR

- Mrs. A, a housewife opens a SB a/c which is later converted into a joint bank a/c with her husband a taxi driver.
- A sudden spurt of income in the current year noted -.
 - 2014-15 Rs.0.50 lacs
 - Current Year Rs.35 lacs
- This does not match with the income profile of the customer in the bank's record.
- The transaction was reported as a STR by the Bank.

Case Study 9 - Cobrapost magazine

- An online magazine Cobrapost conducted a sting on 3 country's leading banks who were found to advise customers on money-laundering.
- shows bankers asking for easily available KYC documents, advising them not to submit PAN to stay off the tax radar.
- Submission of lease agreement & rent receipts as address proof.
- These are suspicious cases, where bank should do a periodic re-check whether the customer still has the same residence or job.
- Cobrapost expose shows bankers allegedly marketing insurance products to convert black money into white because bank earns a high first-year commission on the premium. Bank official rewarded for high sales with foreign junkets.

Best practices

- **Begin with the End in mind**
- Determine customer risk in terms of propensity to commit money laundering, terrorist finance, or identity theft – develop ability to predict with reasonable certainty of the type of transaction likely to be engaged.
- Create expectation of a customer's transactional behaviour
- Monitor a customer's transactions against the expected behaviour & recorded profile as well as that of the customers peer.
- Independent verification of data / information provided by the customer.
- Having a data base of Do not Do Business Clients
- Never failing to meet refresh schedules