



NATIONAL BANKING INSTITUTE

"The Banking Academy Of Nepal"

Best Practices for Fraud Identification Prevention & Mitigation

Seminar on Financial Fraud

NBI & Fintelekt

Kathmandu

March 11,2015

A Presentation by Theresa Karunakaran

- Defining Fraud
- Fraud Risk Management Framework
- Categories of Frauds
 - *Advances*
 - *Technology*
 - *Deposit*
 - *Occupational*
- Best Practices & Strategies for Fraud Prevention, Detection & Mitigation.







AGENDA


FRAUDS THAT SHOOK THE FINANCIAL SYSTEM!

- ❖ 1995-Barings bank-loss of \$1.3 billion in 1995-Rogue trader Nick Leeson
- ❖ 2012-LIBOR Fraud-\$1.5 trillion loss to customers by rigging rates-Barclays settled with regulators for US \$453 million
- ❖ 2012-J P Morgan Chase-London Whale Trader Bruno Iksil -\$2 billion- Settlement cost to JP\$920 million
- ❖ 2011-Citibank Gurgaon India –Rs 400 crore-misselling and diversion of funds from accounts of HNI customers
- ❖ 2012-Deccan Group-Rs 357.00 crore loss-Canara Bank
- ❖ 2014-Fixed Deposit fraud in Dena bank, Oriental Bank of Commerce - Rs 436.00 crore

REPERCUSSIONS OF FRAUD

-  Reputation risk
-  Financial loss
-  Regulatory risk-Penalties
-  Legal risk

FRAUD

 *A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank’.*

Report of RBI Working Group on Information Security,
Electronic Banking, Technology Risk Management and Cyber
Frauds,

INDIAN CONTRACT ACT 1872

Fraud is defined as any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

- ❖ the suggestion as a fact, of that which is not true, by one who does not believe it to be true;
- ❖ the active concealment of a fact by one having knowledge or belief of the fact;
- ❖ a promise made without any intention of performing it;
- ❖ any other act fitted to deceive;
- ❖ any such act or omission as the law specially declares to be fraudulent.

CLASSIFICATION OF FRAUDS

- ❖ Misappropriation & criminal breach of trust
- ❖ Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts & conversion of property
- ❖ Unauthorized credit facilities extended for reward or for illegal gratification
- ❖ Negligence & cash shortages
- ❖ Cheating & forgery
- ❖ Irregularities in foreign exchange transactions
- ❖ Any other type of fraud

KAUTILYA'S DEFINITION OF FRAUD

“What is realised earlier is entered later on; what is realised later is entered earlier; what ought to be realised is not realised; what is hard to realise is shown as realised; what is collected is shown as not collected; what has not been collected is shown as collected; what is collected in part is entered as collected in full; what is collected in full is entered as collected in part; what is collected is of one sort, while what is entered is of another sort.”

Arthashastra-300 BC

FRAUD CASES IN THE BANKING SECTOR

Year	No of cases	Total Amount Rs in crore
2009-10	24791	2037.81
2010-11	19827	3832.08
2011-12	14735	4491.54
2012-13	13293	8646.00
Total frauds reported	169190	29910.12

BANK GROUP WISE FRAUD CASES

Bank Group	No of cases	% to total cases	Amount involved Rs in crore	% to total amount
Nationalised Banks including SBI Group	29653	17.53%	24828.01	83.01%
Old Pvt Sector Banks	2271	1.34	1707.71	5.71
New Pvt Sector Banks	91060	53.82	2140.48	7.16
Sub total Pvt Banks	93331	55.16	3848.19	12.87
Foreign Banks	46206	27.31	1233.92	4.12
Total	169190	100	29910.12	100

ESSENTIALS OF FRAUD RISK MANAGEMENT FRAMEWORK

- ❖ Robust Fraud Risk Management architecture encompassing policies, procedures, internal controls, clearly laid down lines of delegated authority
- ❖ Ownership by Board/Audit Committee of the Board/Special committee of the Board/Top management
- ❖ Enabling organizational culture-high priority on sound operating procedures
- ❖ Systems for monitoring transactions, exposures, events that could be fraudulent –loss to bank
- ❖ **Know your Customer**
- ❖ **Know your Customer's Customer**
- ❖ **Know your Employee**
- ❖ Internal Audit
- ❖ Preventive/corrective action
- ❖ Staff accountability for fraud

CATEGORY OF FRAUDS

- ❖ Advances related
- ❖ Technology related
- ❖ KYC related (Deposit Accounts)

BANK GROUP WISE ADVANCE RELATED FRAUDS

(RS 1 CRORE & ABOVE IN VALUE)

Bank Group	2009-10		2010-11		2011-12		2012-13		Cumulative Total	
	No of cases	Amt	No of cases	Amt	No of cases	Amt	No of cases	Amt	No of cases	Amt
Nationalised banks including SBI	152	736.14	201	1820.12	228	2961.45	309	6078.43	1792	14577.28
Old Pvt Sector Bks	16	99.10	20	289.31	14	63.31	12	49.87	149	767.75
New Pvt Sector Bks	10	63.38	18	234.18	12	75.68	24	67.47	363	1068.18
Sub total Pvt Sector bks	26	162.48	38	523.49	26	138.98	36	117.34	512	1835.93
Foreign banks	4	45.26	3	33.20	19	83.51	4	16.75	456	277.05
Grand total	182	943.87	242	2376.81	273	3183.94	349	6212.51	2760	16690.26

BANK GROUP WISE TECHNOLOGY RELATED FRAUDS

Bank Group	2009-10		2010-11		2011-12		2012-13		Cumulative total	
	No of case s	Amt Rs in crores	No of case s	Amt Rs in crores	No of cases	Amt Rs in crores	No of cases	Amt Rs in crores	No of cases	Amt Rs in crores
Nationalize d banks & SBI group	118	1.82	143	3.39	172	7.26	190	9.85	824	25.60
Old Pvt Sector banks	9	0.15	4	0.46	9	0.06	6	1.09	55	2.30
New Pvt sector banks	14387	34.53	9638	21.41	6552	16.54	3408	33.97	74321	183.48
Sub total	14396	34.68	9642	21.87	6561	16.6	3414	35.06	75200	211.38
Foreign banks	5273	26.88	4486	14.77	3315	14.60	5161	22.45	36455	145.95
Grand total	19787	63.38	14271	40.03	10048	38.46	8765	67.36	111655	357.33

FRAUDS RISK MANAGEMENT IN ADVANCED PORTFOLIO

Best Practices

- ✚ Clearly laid down policies, procedures, levels of delegated authority
- ✚ Rigorous appraisal ,post disbursement supervision and monitoring, risk pricing
- ✚ Checking CIBIL/Credit Information Companies data base-defaulters' list
- ✚ Multiple banking/consortium lending arrangements-exchange of information among lenders
- ✚ Reporting of information on fund based & non fund based exposures of Rs 50 million & above to Central Repository of Information on Large Credits(CRILC)
- ✚ Reporting of Current account balances of customer (debit/credit)of Rs10 million & above
- ✚ Loan Review mechanism- system of Credit audit for large advances
- ✚ Creating charge on securities –legal audit & re verification of title deeds in respect of credit exposures of Rs 5 crore & above
- ✚ Tracking signs of incipient stress-SMA accounts-investigating cases of quick mortality
- ✚ Power of Market intelligence

BANK GUARANTEES

- ❖ Bank Guarantees-Banks should assess financial position of customer ability to repay if invoked-caution in issue of unsecured guarantees
- ❖ Performance Guarantees –banks to be satisfied that customer has necessary experience,expertise to carry out obligations under the guarantee
- ❖ Banks not to issue guarantees to non customers
- ❖ Guarantees to be serially numbered and on security paper
- ❖ Banks while forwarding guarantees advise beneficiaries to check genuineness with issuing bank
- ❖ Guarantees above a cut off of Rs 50000 & above to be signed by two authorised officials jointly

LETTERS OF CREDIT

- ❖ Banks should not extend non fund based facilities/discount bills under LC in respect of beneficiaries who are not their clients
- ❖ LC for import of goods-caution while making payment to overseas supplier on basis of shipping documents
- ❖ Compare clients, check documents to ensure that they are in conformity with terms of LC

FRAUDS RISK MANAGEMENT IN ADVANCES PORTFOLIO

- ❖ Concurrent audit of large branches/transactions
- ❖ Internal Audit role-focus-sampling of transactions
- ❖ End of day exception reports –red flags
- ❖ Caution listing of issuers of certificates where it is established that such certificates were wrong

FRAUDS IN DEPOSIT ACCOUNTS

- ❖ Frauds triggered by laxity in adherence to KYC guidelines
- ❖ KYC non compliant accounts used as conduit for money laundering, routing proceeds of fraud, MLM activities
- ❖ Reputation risk for banks

Know Your Customer

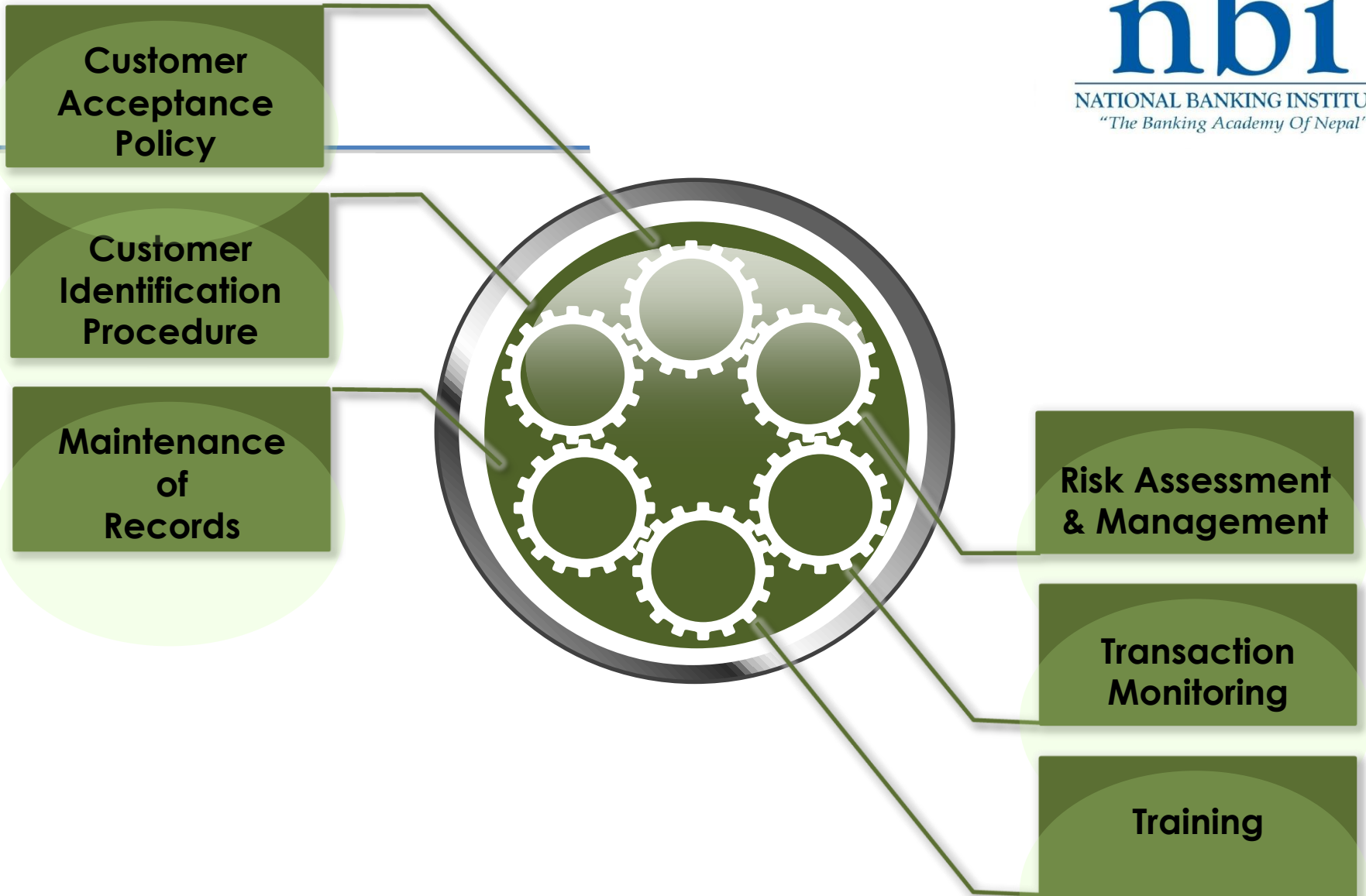
KYC is an acronym for “Know your Customer”, a term used for customer identification process.

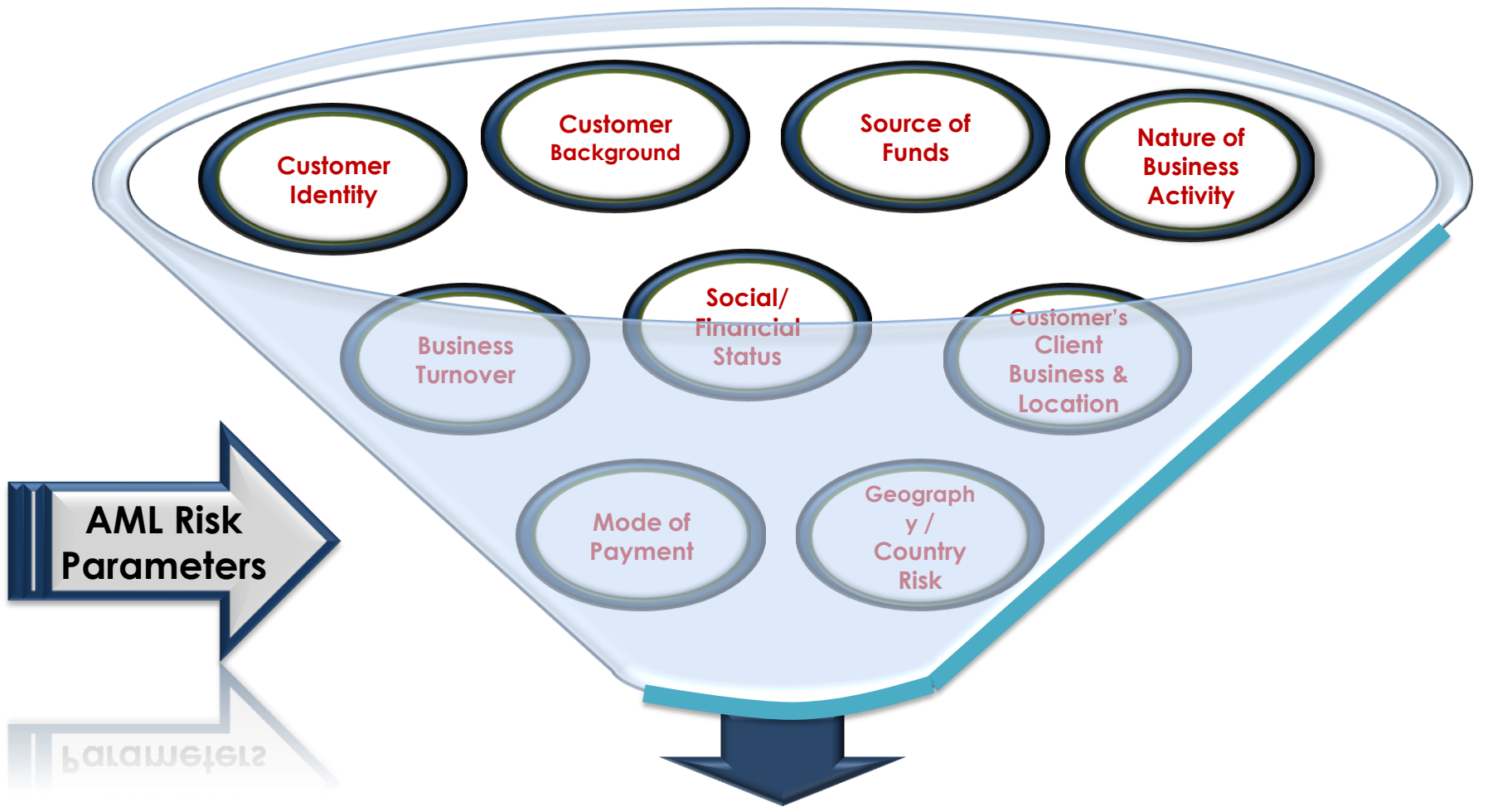
It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc which in turn helps the banks to manage their risks prudently. prevent banks from being used intentionally or unintentionally by criminal elements for money laundering, terrorist activities or fraud

KEY POINTS

- ❖ In India and globally, Regulators have stringent regulations in place
- ❖ India admitted as member of FATF in June 2010
- ❖ Country's financial system judged by standards of its adherence to FATF recommendations
,KYC/AML rules/guidelines adherence
- ❖ Adherence necessary as part of good governance for doing business locally, retaining depositor/customer trust and expanding global footprint.

Core elements of KYC



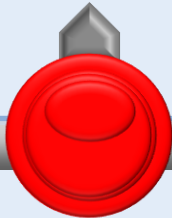


Based on the Above parameters, customers are categorized into three broad Risk Segments

- High Risk** – The customer who can potentially pose higher risk and subject to Enhanced Due Diligence
- Medium Risk** – Customers that are likely to pose a higher than average risk to the bank but are not classified as High Risk, due to other relevant Risk Factors.
- Low Risk** – The customers, whose identities and sources of wealth can be easily identified and apparently carries low risk into system.

Illustrative Examples of Risk Categorization

High Risk Customers



- Politically Exposed Person of foreign origin
- HNI – High Net worth Individuals
- Non-Resident Customers
- Cash intensive business
- Jewellers, bullion / precious metal traders
- Trusts, charities, NGOs and organizations receiving donations
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners
- Non Face to Face Customers
- Those with dubious reputation as per public information available

- Subject to Enhanced Due Diligence
- Requirement of additional documents, on cases to case basis
- Seniors' Approvals in cases like PEP
- High risk accounts are subject to intensified monitoring

Medium Risk Customers



Customers that are likely to pose a higher than average risk to the bank but are not classified as High Risk, due to other relevant Risk Factors.

Low Risk Customers



- Salaried Individuals
- People belonging to lower economic strata of the society
- Government Departments and Government owned companies
- regulators and statutory bodies

the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met

Ongoing Monitoring

On-monitoring is an essential element of effective AML/KYC procedure. The Bank should carry out on-going monitoring of accounts/ business relations of the customers. Such procedure can be broadly classified as under:

- Transaction Monitoring
- Periodic Updation of KYC information and document
- Screening customer data against negative database
- On-going Risk Assessment

TRANSACTION MONITORING SYSTEMS

- ❖ Identification of suspicious transactions is facilitated through the software i.e. FCDMS (Financial Crime Detection Management Suite) based on the alert scenarios configured therein
- ❖ The software is also used for name screening for onboarding and legacy customers against World Check database configured therein.

Transaction Monitoring

Suspicious Transaction Report



Any transaction of suspicious nature, whether cash or non-cash, or a series of transactions integrally connected

STR shall be furnished within **7 days** of arriving at a conclusion that transactions are of suspicious nature

Cash Transaction Counterfeit currency Report

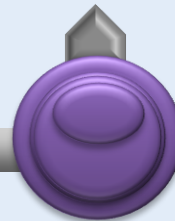


1. Single or series of any value Cash Transactions exceeding total value of INR 10 lakh in a month
2. Forged or Counterfeit Indian Currency Notes used as genuine notes

All such Cash Transactions shall be submitted to FIU-IND on **monthly** basis

Counterfeit currency incident shall be reported immediately

Non-Profit Organization Report



All transactions involving receipts by non-profit organizations of value more than INR 10 lakh or its equivalent in foreign currency

All such transactions in the prescribed format shall be submitted by the **15th** of the succeeding month.

Cross Border Wire Transfer Report



All cross border wire transfers of more than INR 5 lakh or its equivalent in foreign currency

All such transactions in the prescribed format shall be submitted by the **15th** of the succeeding month.

Periodic Updation of KYC information and Risk

Ongoing Name Screening

- To maintain, update the lists of individuals and entities appearing in specified Negative Databases
- Regularly scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in such Negative Lists.
- On receipt of UN sanctions list from RBI, banks to ensure expeditious and effective implementation of the procedures under sec 51 of UAPA
- Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to MHA, RBI, UAPA nodal officer of state/UT and FIU-IND.

Ongoing Risk Assessment

- To monitor transactions of customers based on assigned risk derived from customer profile
- Since profiles and transaction patterns are dynamic in nature, banks are required to assess the customers risk on an on-going basis.
- As per regulator, such review / assessment of risk shall be carried out at a periodicity of **not less than 6 months**.

Periodic Updation of KYC document/ Information

- Re-KYC exercise shall be performed for each customers based on assigned AML compliance Risk
- Such exercise shall be carried out at least at every **10 years** for low risk customers, every **8 years** of Medium Risk customers and every **2 years** for High Risk customers
- Under recent amendments, Regulator has instructed imposing '**freeze**' in phased manner on **non KYC compliant accounts**
- Further regulator also allowed **to close such non compliant accounts**, by giving due notice to customer

RISKS OF NON COMPLIANCE- GLOBAL SCENARIO

- ❖ Standard Chartered Bank [SCB] will pay a \$300m penalty to the New York Department of Financial Services after it failed to remediate transaction monitoring deficiencies in line with a consent order agreed with the regulator in September 2012.
- ❖ HSBC Holdings Plc agreed to pay a record \$1.92 billion in fines to U.S. authorities for allowing itself to be used to launder a river of drug money flowing out of Mexico and other banking lapses in December 2012
- ❖ Credit Suisse paid roughly \$2.6 billion for aiding and abetting US tax evasion. This was equivalent to its net income for 2013
- ❖ BNP Paribas fined \$8.9 million in July 2014 for violation of US sanctions by US regulators for processing billions of dollars through US financial system on behalf of Iranian, Sudanese & Cuban entities

INDIA STORY

- ❖ RBI had imposed penalties in June 2013 for non adherence to KYC/AML guidelines on 3 banks-Rs 10.50 crore
- ❖ July 2013 -22 banks penalized –Rs49.50 crore
- ❖ In August 2013, 6 banks penalized - Rs 6.5 crore
- ❖ July 2014, 12 banks fined Rs1.50 crore for irregularities observed in adherence to KYC and due diligence in lending to Deccan Chronicle
- ❖ December 2014-penalty of Rs 75.00 lakh on 2 banks

TECHNOLOGY RELATED FRAUDS

- ❖ Shift in bank's service delivery platform to mobile, internet, social media, less face to face transactions
- ❖ 65% of cases of frauds were technology related though amount involved was only 1.19% of total frauds
- ❖ Fraudsters tap loopholes in technology systems & processes –use of hostile software programs malware attacks, phishing, Vishing, SMSishing, whaling techniques, stealing customer data to perpetrate frauds

REGULATORY GUIDELINES TO CHECK FRAUDS

Security in card payment transactions

- ❖ Introduction of two factor authentication in case of card not present transactions
- ❖ Conversion of all strip based cards to chip based cards for better security
- ❖ Threshold limits for international usage of debit/credit card
- ❖ Banks to ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS (Payment Applications -Data Security Standards)
- ❖ Frame rules based on transaction pattern of card usage by customers for arresting fraud -Sending SMS alerts

REGULATORY GUIDELINES TO CHECK FRAUDS

Securing electronic payment transactions-through RTGS,NEFT

- ❖ Specific id, password for users
- ❖ Fixing a cap on the value / mode of transactions /beneficiaries-for exceeding cap additional authorisation
- ❖ A system of alert when a beneficiary is added
- ❖ Velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.
- ❖ Consider digital signatures for large value payments say in RTGS
- ❖ Capturing of Internet Protocol (IP) address as an additional validation check

SECURITY ISSUES

- ❖ Peripheral & system security in ATM locations
- ❖ Customer education- do not respond to fraudulent emails/sms messages, part with confidential information PIN, passwords etc

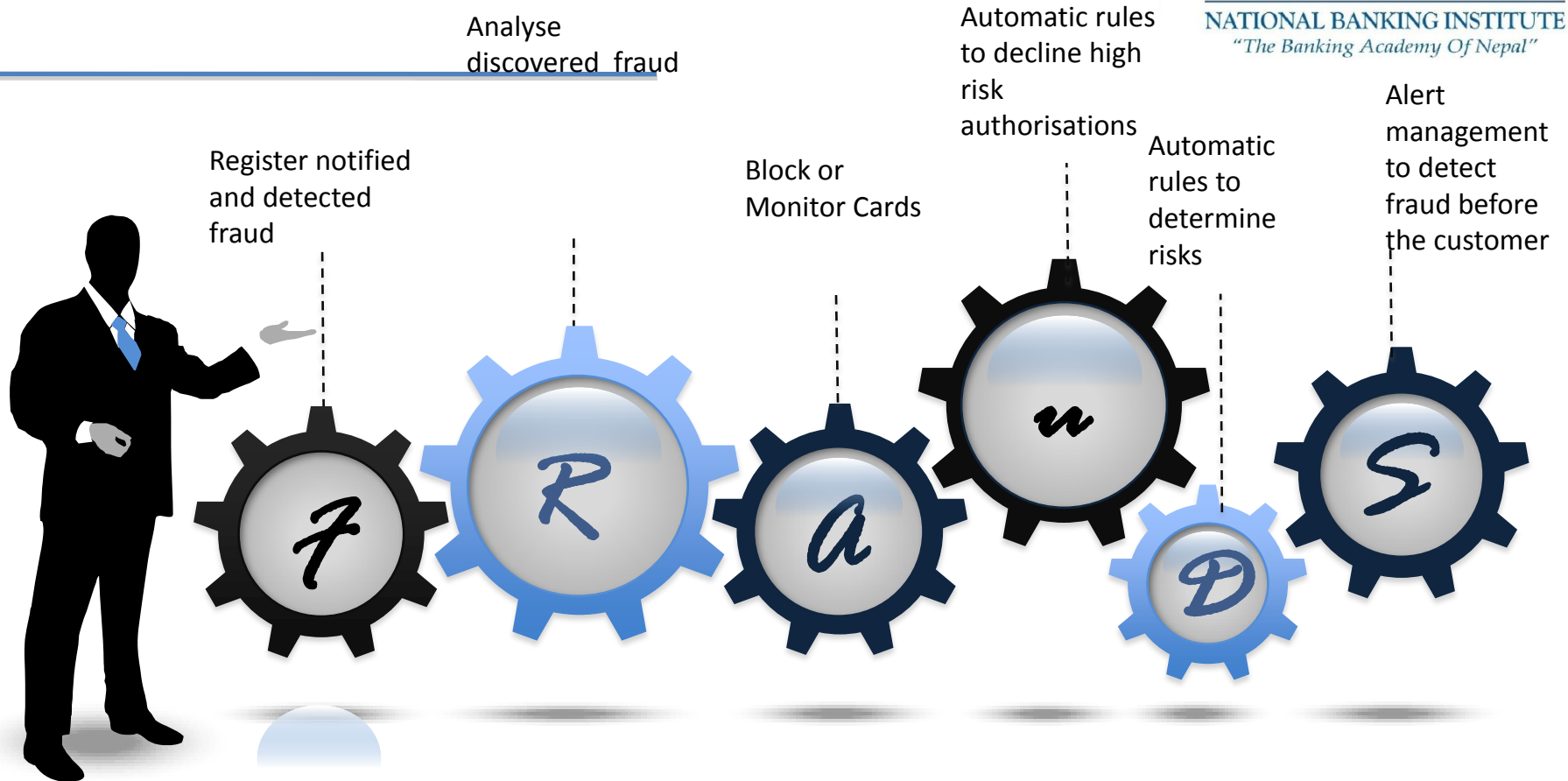
IT SOLUTIONS FOR FRAUD DETECTION & MANAGEMENT

- ❖ Banks are using Clari5 EFM software solutions for monitoring & detecting fraudulent transactions in internet banking space
- ❖ Scenarios for capturing both financial & non financial events-monitoring real time 24 x 7
- ❖ Alerts to customer for transactions, when beneficiary is added
- ❖ Velocity check on number of transactions effected per day /per beneficiary & suspicious transactions alert to the customer & bank
- ❖ IP address as additional validation check
- ❖ Moving to preventive systems to stop/suspend highly suspicious transactions from going through

Credit cards-Objective of Monitoring Transaction



Transaction Fraud Management has many needs :



Falcon Fraud Transaction Monitoring system

What is Falcon Fraud Monitoring ?

1

Falcon is a software, utilized to monitor card transactions for fraudulent activity.

List of Products Monitored

2

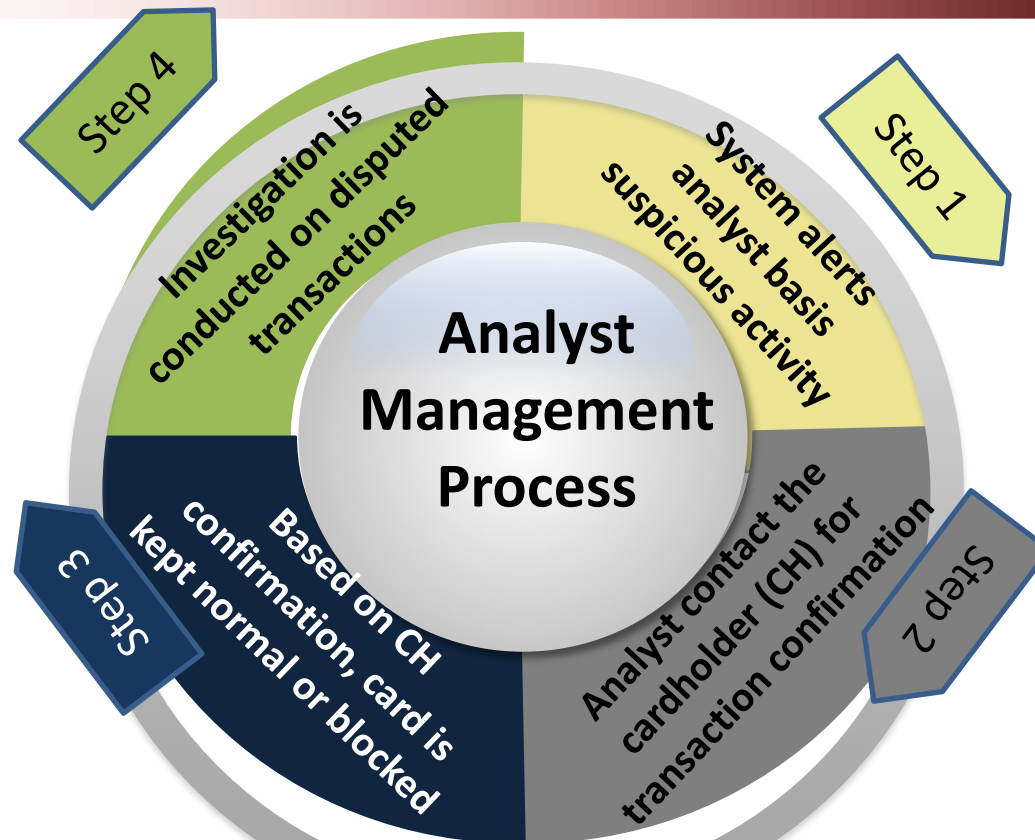
Retail Credit Cards, Debit Cards, on Falcon System.

What types of transactions are considered suspicious or fraudulent?

Falcon monitors and analyses transactions and assigns a score to the transaction. Based on normal spending patterns, if a questionable transaction is detected on debit card or credit card, analyst will contact cardholder to verify the transaction. Falcon can even decline a transaction at the point of purchase if the fraud score is high.

Process and Steps Followed

The Analyst Management Process consists of the following four steps:



Activities at Transaction Monitoring broadly Covers :



nb
NATIONAL BANKING INSTITUTE
"The Banking Academy of India"

Rule Management

- Maintain rules via real time through user interface
- Rules used for case creation.
- Rules are maintained with version controls, audits and change control.

Trigger Management

- Comprehensive Case Management – Monitor both Domestic and International transactions i.e. Card Present and Card Not Present Scenario.
- Review, action and document cases.
- Customizable user interface

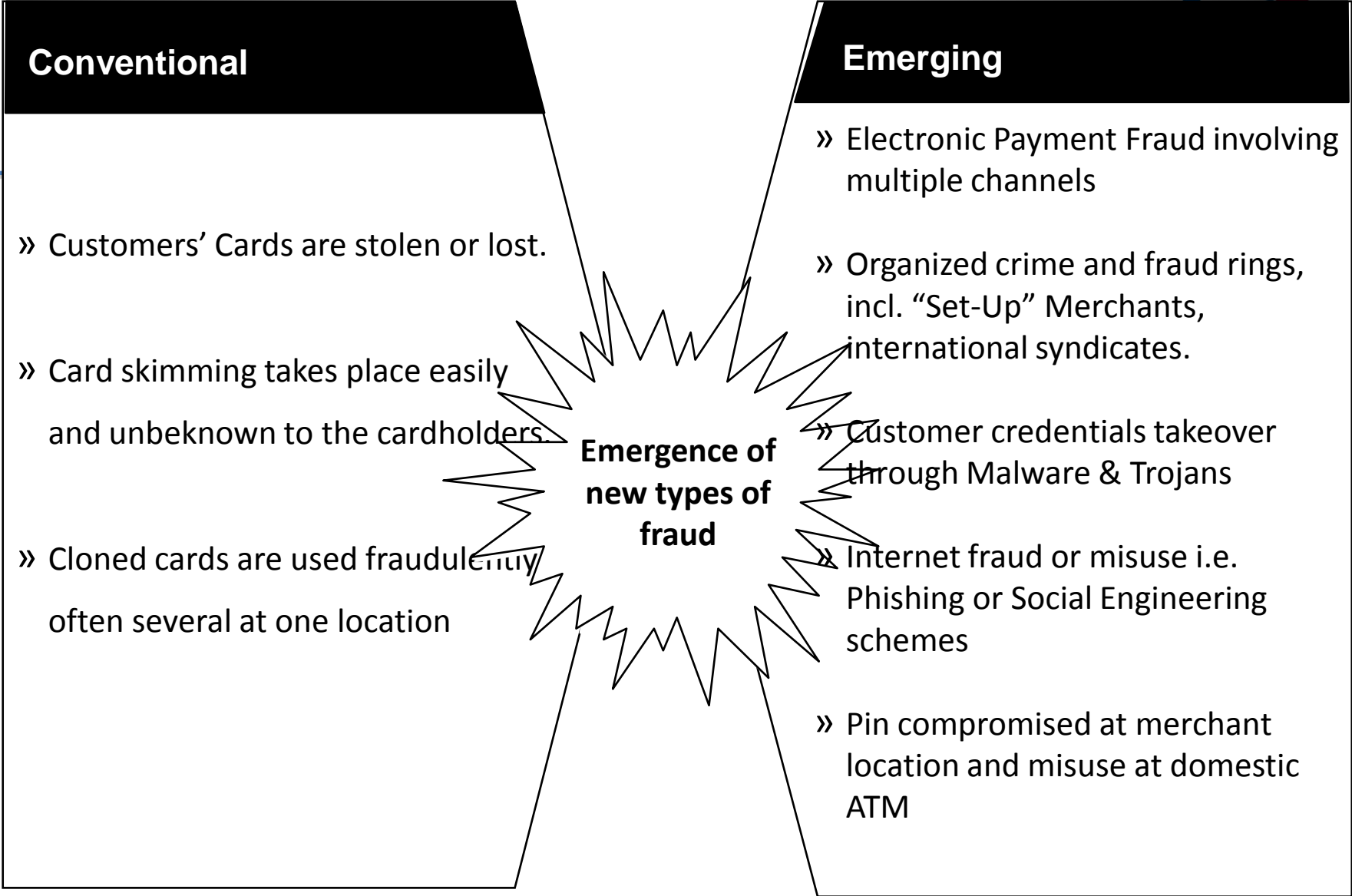
Queue Management

- To trigger all alerts post change in static data change Mobile & E-mail.
- To have flash fraud related rules.
- To have Velocity based rules for POS & Internet
- To have score based rules with multiple variable combinations.
- To have call back related cases.
- Any transaction that has triggered delta threshold.

Process Management

- Audit and Compliance
- Customer Feedback
- Monitoring mechanism to measure Account and Value Detection Rate.

Consumer Banking Fraud is seeing emergence of new types of fraud



TACKLING THREATS TO CYBER SECURITY

- ❖ Unknown cyber attackers stole 76 million customer information from JP Morgan Chase
- ❖ Retail stores Insurance companies in the US were targeted by hackers for customer data
- ❖ Kaspersky Labs a Cyber crime company reported a \$1 billion heist from several banks in Russia,US, Germany ,China,Ukraine by a gang named Carbanak-One bank lost \$7.3 million when its ATMs were programmed to spew cash at certain times that henchmen would then collect, while a separate firm had \$10 million taken via its online platform

TACKLING THREATS TO CYBER SECURITY

- ❖ Firewalls & intrusion prevention systems
- ❖ Guard against malware which gets attached to songs, email messages links-choose safe secure sites addresses-white listing of sites
- ❖ Using tools like Security Incident & Event Management(SIEM), Network Behaviour Anomaly Detection(NBAD)Data Leakage Prevention(DLP) for detection of security breaches
- ❖ Use of data analytics to generate alerts on outlier transactions
- ❖ Use of offsite and real-time monitoring of frauds based on learning insights from historical fraud instances and the current industry landscape
- ❖ Centralized system for fraud monitoring and management of alerts across different systems and data sources
- ❖ Intelligent system along with designed case management to suit the needs of the bank, and thus, prioritize on alerts and areas of greater risk alerts
- ❖ Management oversight through real-time dashboard/MIS to track operational efficiency and monitor fraud investigation findings
- ❖ Make optimum use of the past and current transaction data and fraud Database to make continuous improvements in the dynamic market sphere

Occupational fraud

' Occupational fraud is defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.'

Association of Certified Fraud Examiners' (ACFE)
"Report to the Nation on Occupational Fraud and Abuse 2014"

Involving asset misappropriation, corruption & financial statement fraud

❖ A typical organization loses upto 5% of its revenues each year to frauds ie \$ 3.7 trillion

❖ 22% of cases involved losses of at least \$ 1 million

Occupational fraud

- ❖ Asset misappropriation accounted for 85% of cases with an average loss of \$130000
- ❖ Financial statement fraud -9%-average loss of \$1 million
- ❖ Corruption -37%-average loss \$200,000

INITIAL DETECTION OF FRAUDS



Sl No	Detection	2014 % of cases	2012 % of cases	2010 % of cases
1	Tips	42%	43.3%	40.2%
2	Management reviews	16%	14.6%	15.4%
3	Internal Audit	14.1%	14.4%	13.9%
4	By accident	6.8%	7.0%	8.3%
5	Account reconciliation	6.6%	4.8%	6.1%
6	Document Examination	4.2%	4.1%	5.2%
7	External Audit	3.0%	3.3%	4.6%
8	Surveillance Monitoring	2.6	1.9%	2.6%
9	Notified by law enforcement	2.2%	3.0%	1.8%
10	IT Controls	1.1%	1.1%	0.8%
11	Confession	0.8 %	.5	1.0%
12	Others	0.5%	1.1%	

LESSONS FROM THE STUDY

- ❖ Tips are consistently the most common detection method
- ❖ Organizations with hotlines are most likely to detect a fraud
- ❖ Where anti fraud controls have been implemented loss has been lower and detected more quickly
- ❖ Controls include proactive data monitoring & analysis, surprise audits, dedicated fraud department or team, formal fraud risk assessments, ongoing employee monitoring

HR STRATEGIES

- ❖ Know your employee
- ❖ For key & sensitive posts like Treasury, dealing room, heads of specialised branches, RMs for high value customers - identify officers who satisfy fit & proper criteria
- ❖ Rotation of staff, mandatory leave

KEY TAKEAWAYS

Fraud Risk Management Framework

- ❖ Robust Fraud Risk Management architecture encompassing policies, procedures, internal controls, clearly laid down lines of delegated authority
- ❖ Corporate governance-Ownership by Board/Audit Committee of the Board/Special committee of the Board/Top management
- ❖ Enabling organizational culture-high priority on sound operating procedures
- ❖ Internal Audit

Best practices for fraud prevention, detection and mitigation in :

Advances

- ❖ Clearly laid down policies, procedures, levels of delegated authority
- ❖ Rigorous appraisal , risk pricing ,post disbursement supervision and monitoring, credit audit, legal audit of documents tracking signs of incipient stress ,market intelligence

Deposits

- ❖ Know Your Customer –compliance with AML Rules

KEY TAKEAWAYS

Technology related frauds

- ❖ Securing internet banking, card transactions through pass words, two factor authentication, use of chip based cards, threshold limits for international usage of credit/debit cards,
- ❖ Use of technology to monitor transactions and prevent fraud
- ❖ Frame rules based on transaction pattern of card usage by customers for arresting fraud - SMS alerts to customers
- ❖ Customer education
- ❖ ATM security
- ❖ Cyber security-Firewalls & intrusion prevention systems, technology to detect security breaches , generate alerts for outlier transactions

Occupational Fraud

- ❖ Know your employee
- ❖ HR strategies-posting employees who satisfy 'Fit & proper , ' criteria to key posts, job rotation ,mandatory leave.

AND LASTLY

 Be ever vigilant!

Thank you!

