PREVENTION AND DETECTION OF BANK FRAUDS

V. Rajendran
http://venkrajen.in
venkrajen@yahoo.com

044-22473849; 9444073849

Contents and concepts

- Bank Frauds: definition and the concept
- Financial frauds and economic offences
- Types of bank frauds –Modus Operandi
- Physical delivery channels and e-delivery channels
- Impact of computerisation in the bank fraud scenario
- Detection of bank frauds – Inspection, Audit, reports
- Prevention of bank frauds – regulatory compliance
- Awareness initiatives – the different stake holders
- The road ahead …….

Crime scenario in banking

- Evolution of banking:
  - Nationalisation (and then Privatisation??)
  - Globalisation
  - competition
  - foreign banks
- Entry of technology – Computerisation
- Re-definition of bank frauds – tech-based, e-offences
- Technology penetration in banks: Customer relationship
- Exposure to computers: exposure to frauds in banks?
- Entry of cyber crime in banks - the inevitable?

What constitutes a bank fraud

- Security: Being free from danger, defence against failure, Freedom from anxiety, safeguarding assets
- Safety, freedom, protection: *of* (Assets) *from* (individuals and threats) *against (*loss, injury etc)
- Information Assets and other assets in a bank
- Infringement of others' rights – Data theft, Data loss
- Financial loss to customers:

Role of banks and as custodians, sometimes they are the victims and sometimes the accused too …. ….. …… …. *Where lies the distinction*?

Crimes associated with bank frauds

- Economic offences involving banks
- Money Laundering (banks as an accused or a victim)
- Cheating, forgery, Cheque bounce cases
- Cyber Crimes like
  - data diddling and data manipulation
  - Password theft and id theft, key loggers etc
  - Access Control and Privileges
  - Internet Banking frauds like DoS Attacks, virus, Trojans
  - ATM frauds like skimming, Card theft, Card clining
  - Credit card frauds like card thefts
  - Mobile banking frauds – data in transit

Types of bank frauds

- Traditional frauds –
  - forgery: customers' or supervisory officials' or colleagues' signature
  - manipulation of accounts: inoperative accounts, NRE accounts, other branches', in transit, sundries, fake bills
  - loans and advances: fictitious persons or assets, fake documents, inflated valuation, diversion and faked losses
- Frauds in a computerised environment
- Insider involvement with a third party
- Frauds due to lack of supervisory controls and inadequate or lack of systems and procedures

Delivery channels in Banking

- Physical delivery channels – Physical thefts in banking, theft of cash, loss of records, physical crimes like assault or burglary etc
- Security concerns in Core Banking environment: centralised data, access from different places etc
- Electronic Delivery Channel in Bank (as opposed to personal channels) like
  - ATMs, Cards, E-Banking, Mobile Banking
- Significance of such channels (Alternate channels)
- Security concerns in all these …

Detection of bank frauds

- Internal inspection: regular or surprise, periodical, HO/ Central Office, Information system audit, RBI etc
- Reported by: customers, colleagues, evidences seen etc
- Failed advances and non-performing assets
- Staff disciplines and lack of procedures
- Trade Union and related employees' activities
- Routine reporting of statements and reports to HO etc
- Accidental and '*by-chance*' detection of frauds

Prevention of bank frauds

- Follow the systems and ward off frauds!
- Systems and Procedures - in the particular bank, in the industry, government's rules, local guidelines etc
- Compliance issues: Consequences of non-compliance like penalty, cancellation of licences, criminal action
- Constant review of crime scenario in the bank
- Compare with the peer-level banks in the industry
- Post incident review and preventive methodologies
- Periodic review of security incidents – reports analysis

Regulator - RBI

- DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01 dated June 14, 2001 addressed to all Scheduled Commercial Banks on Guidelines on Internet Banking in India sets out in detail instructions for adherence classified as
- Technology and security standards
- Legal issues
- Regulatory and Supervisory issues
- RBI's earlier circular RBI/2005-06/71 DBOD No. Comp.BC.14/07.03.29/2005-06 dated July 20, 2005

RBI - Gopalakrishna Working Group

- On I.T. Governance: I.T. Policy, I.T. Steering Committee, define key focus areas, Board powers, identify C.I.O., IT Infrastructure etc
- On I.T. Security: Risk Management, CISO, Information Assets, role of IDRBT, CERT-In, ISO27001 implementation, 2-factor, OTP etc
- I.T. Operations be part of bank's goals
- I.T. outsourcing: monitor and regulate
- I.S. Audit Policy: Formulate, implement, monitor
- Cyber Frauds, BCP, Customer Education, Legal Issues

Investigation of cyber crimes

- Investigation of a bank fraud: civil and criminal
- Bank's Management side investigation
  - Internal Inspection
  - Verification of specific instances
  - Periodic inspection
  - Vigilance and Disciplinary Action Cell
  - Fraud Containment Cell – Routine actions
- Bank's role in police investigation
- Bank's co-operation with the police:

  Duty-bound to co-operate….

Evidences in bank frauds scenario

Thanks to the I.T. Act 2000, records can be maintained in electronic form; are valid records

Onus on the part of banks to maintain records in e-form and to present the same in an acceptable, legally valid and as irrefutable evidences

Maintenance of logs and trails especially in a CBS environment with multiple accesses

Logs and records kept with a third party like intermediaries like ISPs, NSPs etc which serve as valid evidences in instances of bank frauds

E-Record Maintenance Policy in banks – nascent stage?

Bankers Book Evidence Act 1891

- Sec 2 clause 3 Bankers Book includes ….whether kept in the written form or as printouts of data stored in floppy….
- Sec 2 clause 8 (a) certified copy means…copy of any entry certificate at the foot of such copy ….and (b) consists of printouts of data stored in a floppy with certificate in accordance with the provisions of sec 2A
- 2A conditions in the print-out as detailed in (a), (b) A to I and (C)

Reserve Bank of India Act 1934

Regulation of funds transfer through electronic means between banks or between banks and financial institutions

Indian Penal Code 1860

- Sec 4 any person …beyond India committing offence targeting a computer resource located in India…..
- Sec 118 and 119 voluntarily conceals, by any act or illegal omission *or by the use of encryption or any other information hiding tool,* the existence of a design…
  - Sec 464 'digital signature' replaced by 'electronic signature'

The Indian Evidence Act 1872

Sec 3 electronic signature

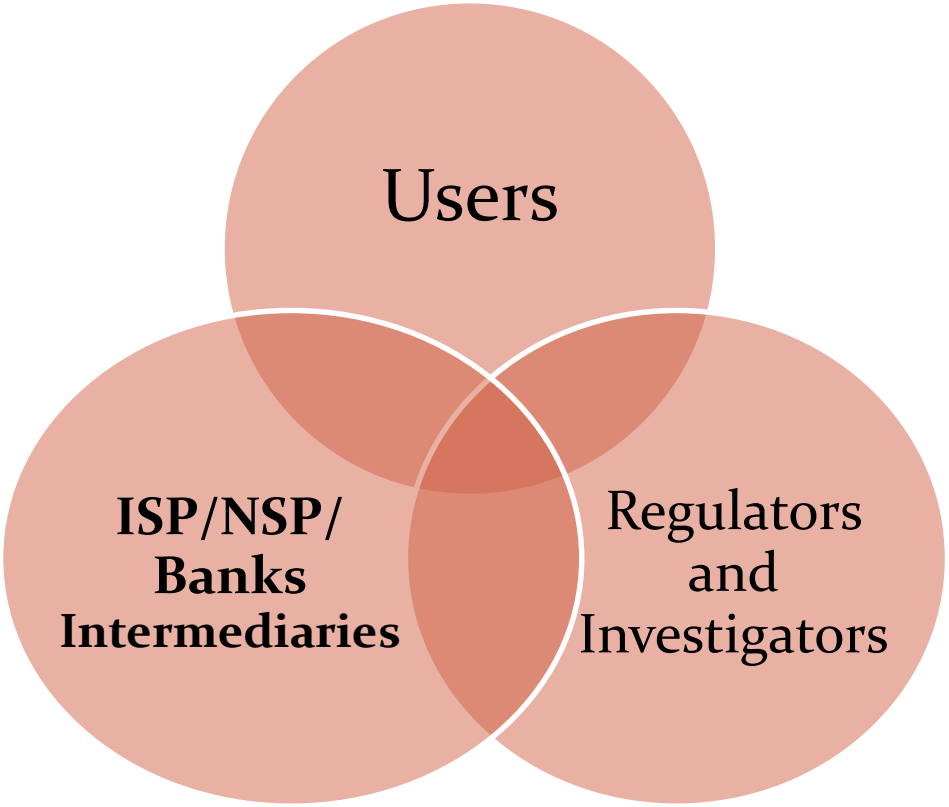
Sec 45A Opinion of examiner of electronic signature – expert

47A and other sections electronic signature replacing digital signature and certificate…

Prevention of Money Laundering Act, 2002

- What is Money Laundering as per the Act?
- Every banking company required to maintain record of all transactions, of the nature and value specified in the rules…furnish information…identity of clients
- Central Government has framed rules
- Cash Transactions 10 lakhs & above or those involving fake or counterfeit notes or all suspicious transactions
- Punishment for bank officials defined
- Necessity to maintain records (e-records), as per procedures framed by RBI and SEBI

The three stake holders in fraud prevention



Questions ???

Thank you.....

V. Rajendran
www.http://venkrajen.in
venkrajen@yahoo.com
044-22473849; +91-9444073849