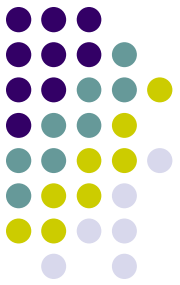
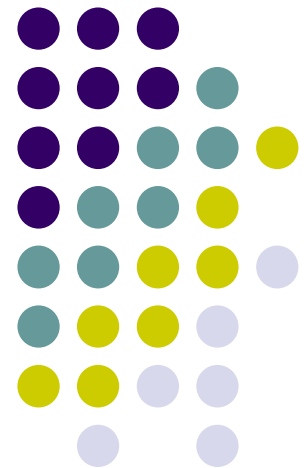


# ATM Frauds Telecom Frauds



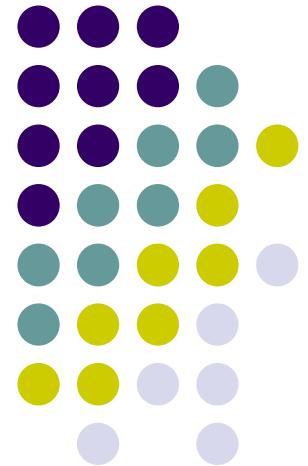
V Rajendran  
venkraj@yaho.com

- Evolution of banking
- Nationalisation
- Post nationalisation era
- Privatisation and Globalisation
- Private sector banks
- New Generation Banks
- Evolution and Revolution
- Banking redefined
- Banking Channels

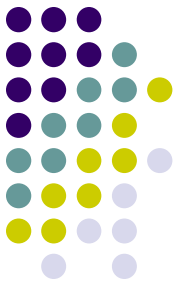


# Electronic Banking Delivery Channel:

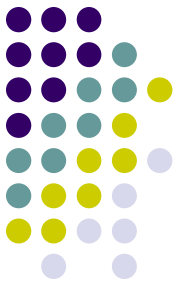
- ATMs
- Internet Banking
- Debit Cards, Credit Cards, Smart Cards
- Mobile Banking
- Other Utility Payments
- RTGS, NEFT and other payments



# ATMs –Concept and Definition



- History and Genesis of ATMs
- Definition of ATMs
- Advantages of mechanisation and automation
- Benefits of Computerisation and network
- Reasons for popularity of ATMs
- Cost factor
- Human Factor
- Social factor
- Cultural and psychological factors



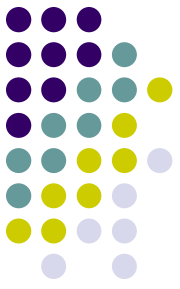
# ATMs –Types

- Based on location:
  - On-site and Off-site ATMs
- Based on functions:
  - ATMs and Cash Dispensers
- Based on connectivity:
  - On-line and Off-line ATMs



# ATMs Frauds

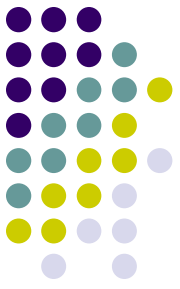
- Spying while entering PIN
- Tailgating while entering the ATM cabin
- Physical theft of ATM Cards
- Non-reporting of loss of ATM Cards
- Bank staff members' abetment in crime
  - Handling of ATM Cards before despatch
  - Handling of lost and misplaced cards
  - Handling while renewal of cards
- Third Party volunteering to help: Lebanese Loops
- Outsourced agency for ATM maintenance



# Common ATM frauds and solutions

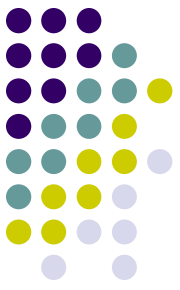
- Physical loss of cards/cash – Alertness, Care
- Hardware issues: Cards struck etc -- Vendors
- Software issues: dispenser, debits -- Vendor/Bank
- Mis-use of cards and PINs -- Use bio-metric
- Disgruntled Staff of the Bank -- solution ??
- Gullible customers -- customers be alert
- Ignorance of customers, staff -- Training
- Skimmers and other devices -- Alertness

# ATMs Frauds -Remedies



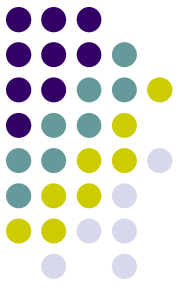
- Monitoring mechanism by banks:  
Video Surveillance, security guards, logs, biometric devices, bullet proof filming, safety of ATMs
- Customers be alert  
Use of PINs and passwords  
Physical possession of cards  
Reporting of loss of cards
- Issuing bank's responsibilities  
Despatch of cards, PIN mailers, bank's custody,  
Cash Management, Database issues,  
reconciliation issues (especially in a consortium)





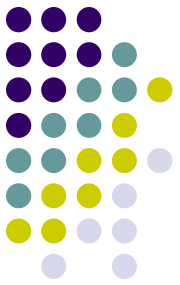
# ATMs Frauds – Administrative issues

- ATM Consortiums: Present Position
- Inter-bank reconciliation issues
- Fraud prone areas in inter-bank transactions
- Cash handling and Account Services: inter-bank
- Outsourced Maintenance Services:
  - Effective SLAs, Penalty Clauses, down-time assurances given, Fall-back options
- RBI and other regulatory measures
- Surveillance mechanisms:
  - Physical (CCTV etc) and logical (trail, logs etc)
- Reporting and compliance issues



# Payment through Cards

- PoS Terminals and their uses
- Card Verification -- Customer identification
- Merchant's responsibility
- Bank's Agreements with the merchant
- Marketing of cards by Third party firms
- Swiping devices -- Skimmers
- Duplicate Cards -- skimmed cards and use
- Ensure card is swiped only once and in the authorised device only



# Other types of cards

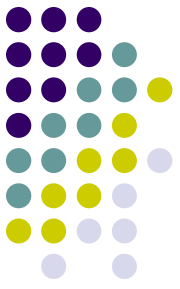
- Credit Cards
- Debit Cards
- Visa Cards
- Master Cards
- Smart Cards
- Other merchant Cards
- Security Issues:
  - Identification: Photo, Signature, others



# Security - The 'Card'inal principles

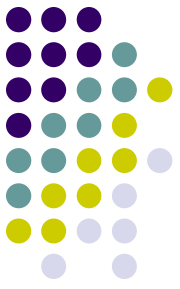
- Merchant's responsibility verify sign, photo
- CCs with PIN authentication – new concept
- Inform Card Loss to the Bank
  - Bank's 24 x 7 Help-desk
- Dealing with captured cards
- Dealing with cards to be issued:
  - at the Card Managers' Desk
  - at the bank's premises
  - at the courier office

# Telecom Frauds

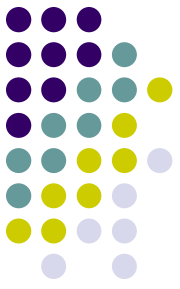


- Definition of telecom fraud: Normal frauds, cyber fraud and specialised ones like telecom fraud - Unauthorised use of telecom facilities and illegal and unlawful use of telecom resources
- Billing frauds: Software-based- Salami techniques
- Cyber Terrorism
- Cyber stalking
- Hoax mails and related offences
- Hacking data networks, hacking PABX etc
- Data theft
- spoofing
- 'Vishing' like Phishing

# Telecom Frauds - Remedies



- Securing the Voice infra-structure
- Management Commitment: Awareness
- Employee and employer's Accountability
- Logs and reports and trails
- Preservation of logs for investigation purposes
- Compliance: Legal and social obligations
- Security Audits of the organisation
- Conformance to Security Standards: BS 7799 and ISO 17799 with 27001 certification
- Internal Security Policy and its compliance

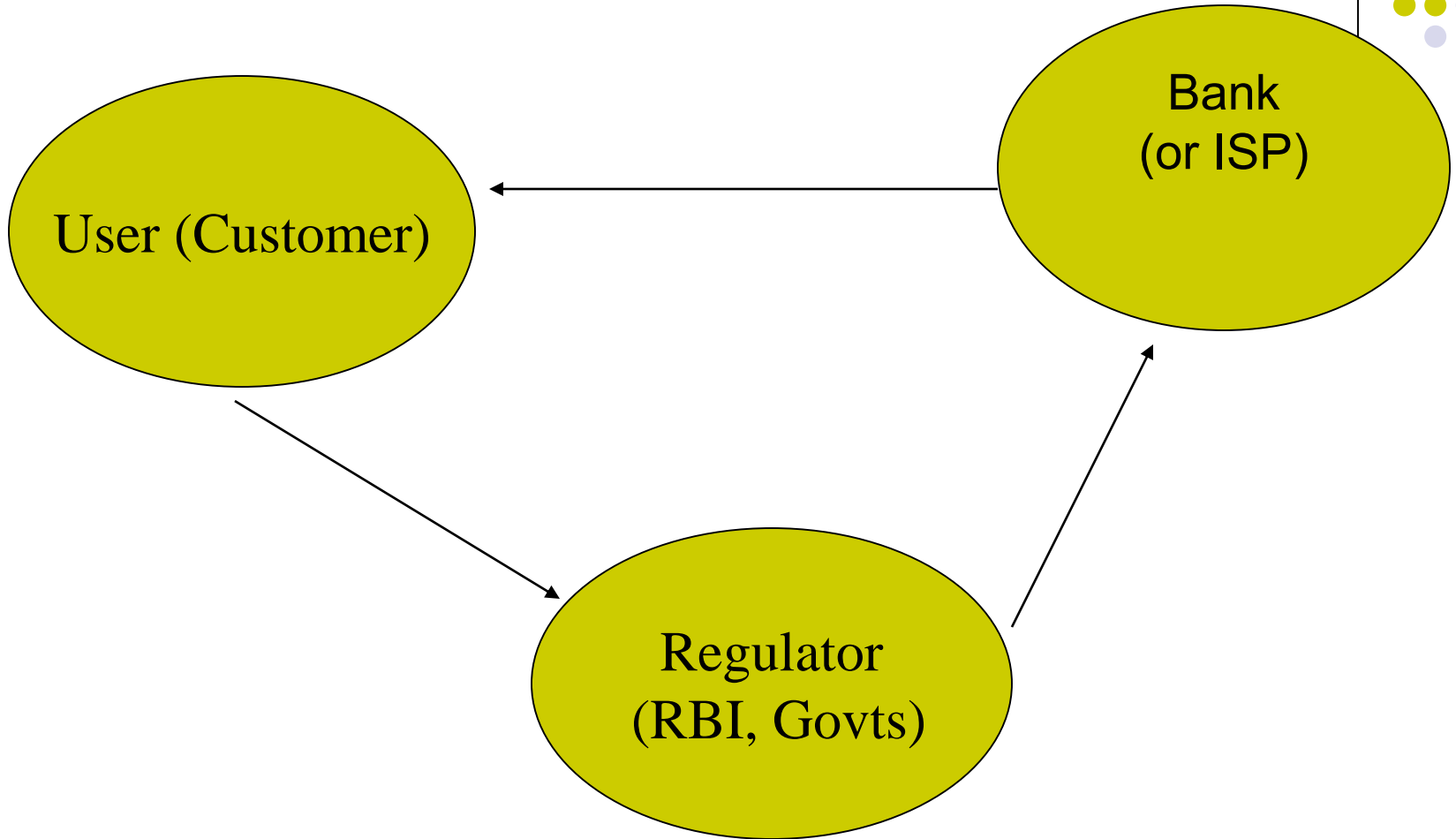


# Cyber Crime - Investigation

- Difference in investigation methodologies
- Knowledge of computers: Domain knowledge
- No scene of crime
- No marking or locking of crime spots
- Time is the essence
- Volatility of a cyber offence
- Investigation methodologies
- Evidence gathering and production of evidences
- Legal and judicial scenario in a cyber offence

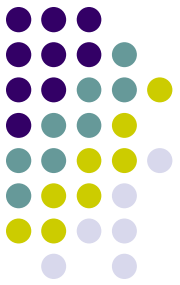


# General Safeguards





# Questions ???



Reach Me  
[venkrajen@yahoo.com](mailto:venkrajen@yahoo.com)

Thank you.....