CBS – Interfaces and Electronic Delivery Channels

V. Rajendran

Advocate and Cyber Law Consultant

URL: venkrajen.in

venkrajen@yahoo.com, rajcyberlaw@gmail.com

+91-44-22473849; +91-9444073849

Technology era in Banking

- Genesis and growth of banking
- Banking Nationalisation: Service Motive
- Globalisation, privatisation: Profit-making
- Entry of private sector banks
- New Generation banks
- Technology in banks: ALPM, TBA to CBS
- What CBS did to banking industry
- Technology based banking products
- Physical delivery channels and electronic delivery channels

E-Delivery channels in Banks

- Evolution of Banking in India
- Evolution of computerisation in banking- competitive edge
- Physical delivery channels and e-delivery channels
- ATMs, Internet Banking, Cards and Mobile Banking
- The common threats: Phishing, Vishing, spam
- Insider threats – disgruntled employees
- E-crimes: Key-loggers, cloning, skimming, spy cameras
- Id theft, Social engineering
- System-based risks: network based, server level data thefts
- *CBS – convenience to customers and staff, but information (in)security?*

Technology in Electronic Delivery Channels in Banks

Need for an e-Delivery Channel?

Features – Necessity or an enabler?

Replacement for human/personal channel?

Security enhancement or security threats?

Security initiatives in such channels benefit

Customer? Bank staff? Industry? Government?

Security and Ease of Use – Strike a balance

Technology and security in ATMs

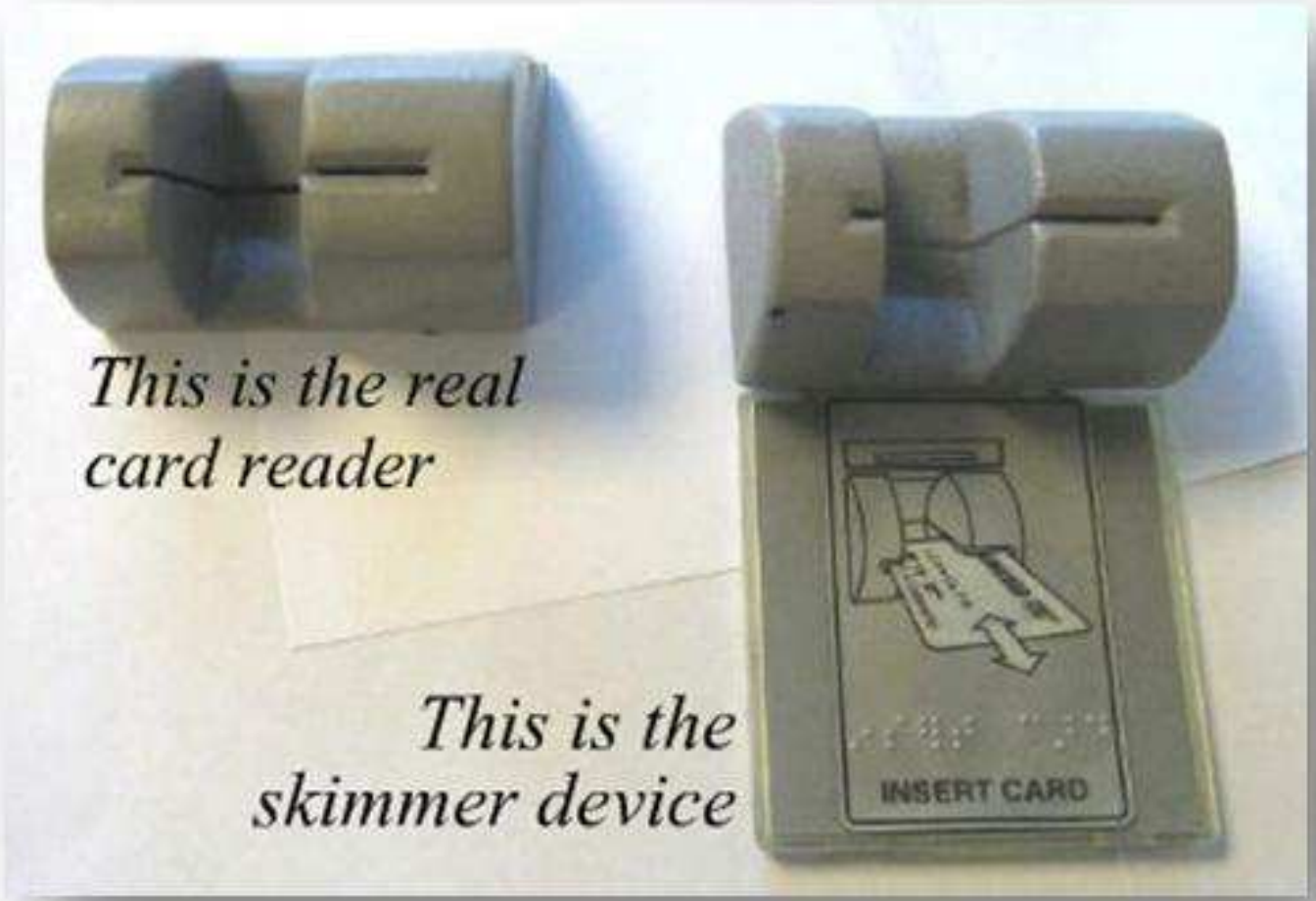
- Physical security: Security Guard, Upkeep, Cash loading and cash movement, CCTV, surveillance, fake notes in ATM, Cash holding limit, skimmer machines in an ATM, Lebanese loop
- Security in an off-site ATM: Cash, Upkeep
- Logical security: Access Control, PIN Validation, impersonation, id theft, tailgating, Software upgrades, Remote Access
- Bio-metric enabled ATMs - experimental

Role of PIN in ATMs

- Two factor authentication in ATM transactions
- How the PIN is generated by the server
- How does the PIN travel from the server
- Concept of natural PIN, hash value, offset value and PIN generation – Natural PIN
- How the PIN is stored in the server
- Security issues in PIN and other ATM transactions

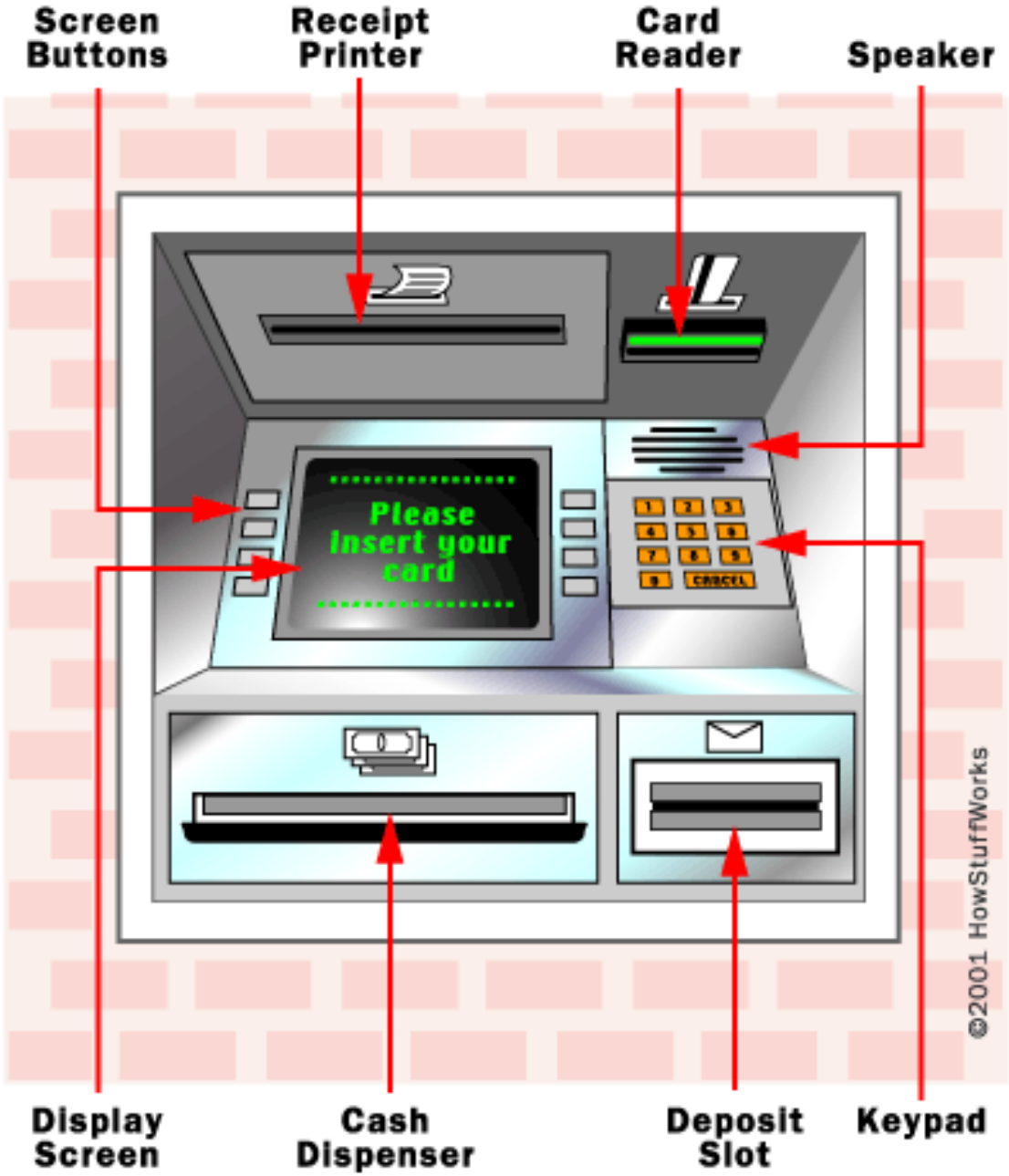
Security issues in ATM

- Dealing with ATM cards at the bank
- Surrendered cards, new cards to be issued etc
- Lost and misplaced cards, procedural issues
- Log of ATM transactions
- Controls in ATM log maintenance
- Interpretation and understanding of ATM logs
- Banks' Info Security Policy on ATMs and the entire security architecture around ATMs


This is the real
card reader
This is the
skimmer device
INSERT CARD

1. ATM Interior

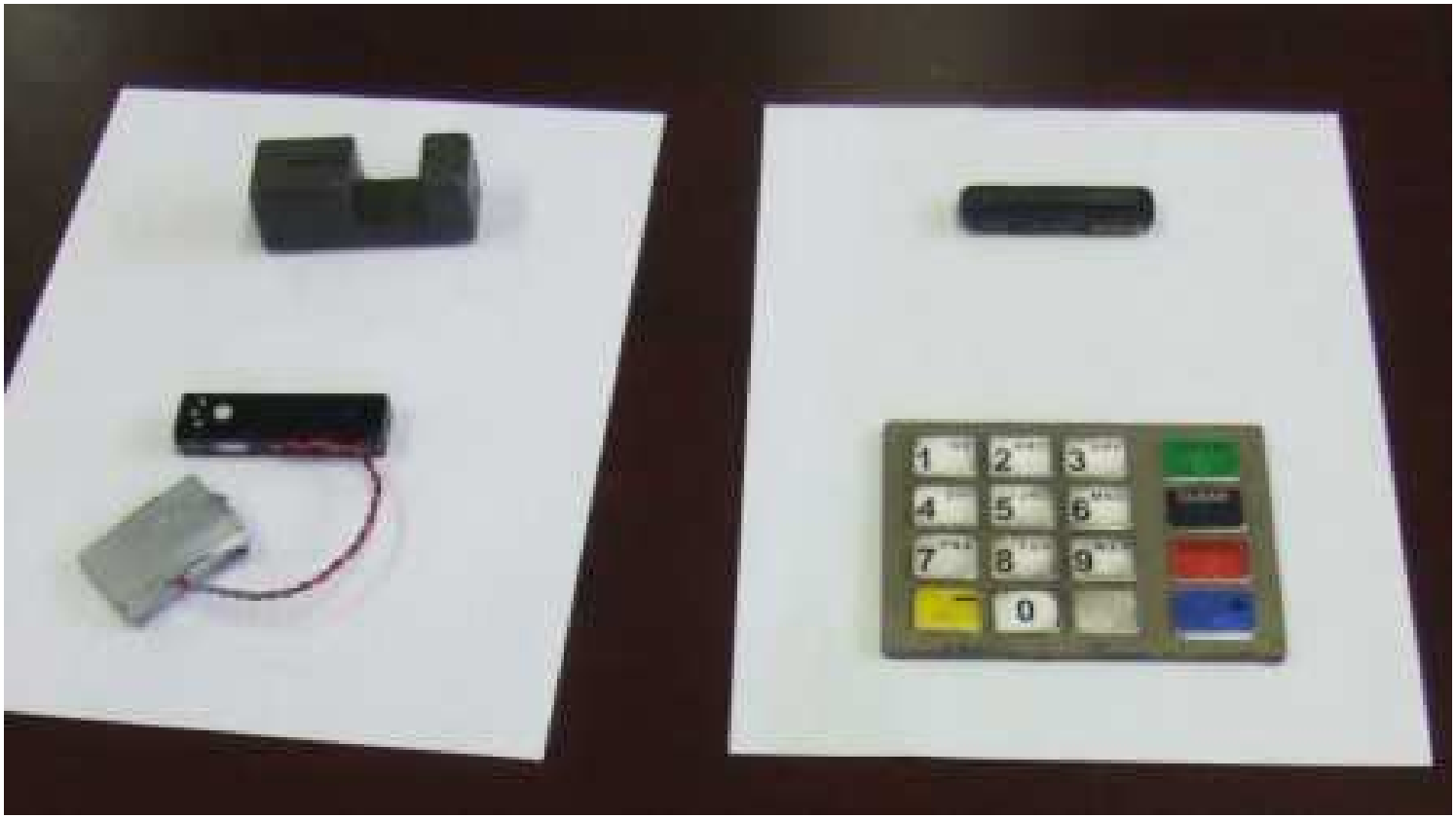
2. Small Fancy ATM


Screen Buttons
Receipt Printer
Card Reader
Speaker
Please Insert your card
CANCEL
Display Screen
Cash Dispenser
Deposit Slot
Keypad
©2001 HowStuffWorks

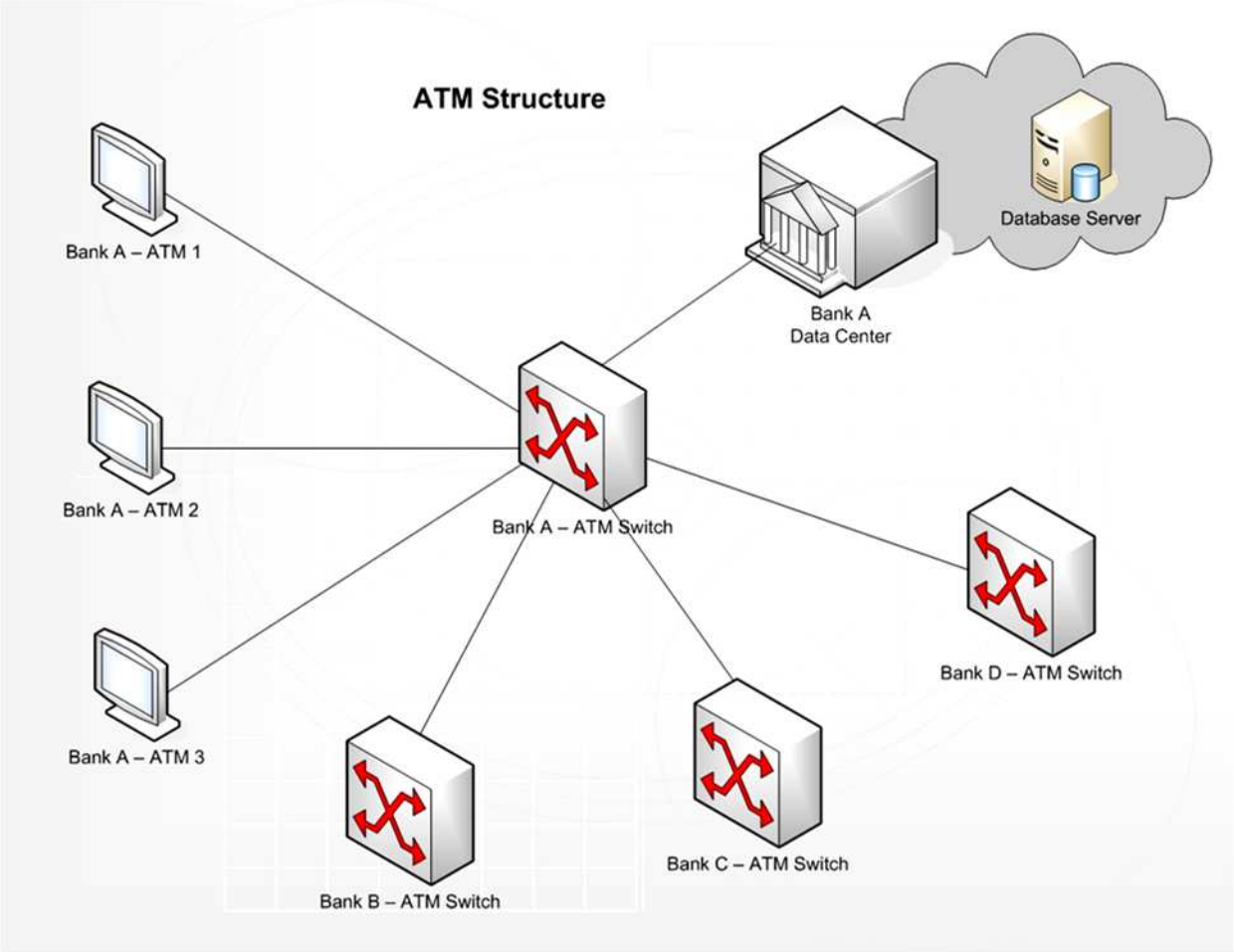
Most common ATM frauds and solutions

- Physical loss of cards/cash – Alertness, Care
- Hardware issues:
  - Cards struck etc – solution from vendors
- Software issues
  - dispenser failure, debits not reversed in time etc
- Mis-use of cards and PINs
  - -- Security at the banks – Despatch of ATM cards and PIN mailers
- Disgruntled Staff of the Bank -- solution ??
- Gullible customers -- customers be alert
- Skimmers and other devices – Alertness

Tampa police show a skimming device — the false card slot goes over the original; underneath is a card reader that captures information. A camera is typically hidden on the ATM, often in a pamphlet holder, angled to view the monitor and keypad. Source: Internet



ATM Structure



Verification of PIN

- Customer insert card & enter PIN
- Encrypted PIN sent to ATM Switch
- ATM verifies card details from database & confirm correctness
- Natural PIN generated
- Switch is having the value which is difference between actual PIN & natural PIN
- This offset value verified using HSM/SSM
- If tallied customer/card is authenticated

Evaluation of Controls in ATM

- Card & PIN generation process
- Dealing with surrendered card
- Security of PIN
- Control over cash
- Maintenance of transaction records
- Dealing with lost/ stolen cards
- ATM Switch operations

Card & PIN Generation

- Separate department to handle card & PIN
- Confidentiality in PIN mailer generation
- Reconciliation of no. of PIN mailer & card produced
- Physical & Logical access control
- Flow of data to card printing agency, if outsourced
- Stock of blank cards
- Control on card card embossing & PIN mailer
- PIN & card should be despatched separately by different courier
- Record maintenance
- Handling of returned cards

Surrendered & Captured Cards

- Complete documentation
- Process for replacement of card & PIN
- Process for making captured card ineffective
- PIN mailer need not be returned by customer
- Register for surrendered card
- Removal of captured card on regular basis
- Report from Data Centre & reconciliation
- Capture procedure for entering wrong PIN thrice

Security of PIN

- Report by customer- block immediately
- Not to disclose PIN to anyone
- Process of timely generation of new PIN
- PIN/PIN offset should always be in encrypted form
- HSM/SSM should be in self destructive mode
- All storage for PIN encryption should be zeroised after each calculation
- No hard copy of record of PIN produced

ATM cash Management

- Documented procedures for cash balancing
- Journal should automatically record all withdrawals
- Cash inserted in each BIN/ cassette should also be recorded
- Cash reconciliation for cash dispensed, remaining cash, misfit notes
- All discrepancies noted & reported
- Maintenance of cash & reconciliation by 2 different persons
- Wrong denomination – should be doubly check
- Daily balance procedure

Security in ATMs

Physical safety of ATMs

- Monitoring mechanism by banks: Video Surveillance, security guards, logs, bio-metric devices, bullet proof filming and other measures
- Customers: Be alert – Security concerns use of PINs and passwords – Physical possession of cards and preservation of PIN
- Issuing bank's responsibilities: Despatch of cards, PIN mailers, bank's custody, Cash Management, Database issues, reconciliation issues

ATM – the Technology

- ATM Server stores the account holder details
- ATM App Server – its role in CBS
- ATM Switch in banks – its role
- Visa Switch Master Switch etc – Common switches
- Account holder's file sent to ATM Switch – **PBF**
- Interaction of ATM Switch with Central DB Server
- Security concerns in the ATM data flow

ATM – e-Records

- Meaning and purpose of electronic journal
- ATM Journal – Logs and Trails
- Preservation of ATM logs: At the switch, at the server, at the branch, at the ATM
- CCTV footages – Preservation and retrival
- E-Records as evidentiary value
- ATM Audits: Verify records, editability of logs, preservation, card and PIN verification, PIN and emailer generation, security concerns

Technology in Internet Banking

- Definition
- Most convenient, from home, any time..
- query-based and actual transactions
- Other facilities offered: funds transfer, statements, cheque book requests etc
- Authentication: username and password
- Internet Banking App Server
- Internet Banking DB server
- Interaction with the bank's DB Server

Cyber Crimes – e-banking

- Never from a browsing centre, cyber café or any public place
- Always look for security features like
- lock symbol
- **Green Address bar - EVSSL**
- Site Certification details
- Beware of key-logger software – Use of virtual keyboard
- Beware of phishing mails and phishing site
- Never reveal any information (user-id password) over email
- Never click any hyperlink in any website and give info

No bank will ever require any info by email

In addition to the CVV-CVC, remember the t-PIN (additional PIN auth-PIN) for e-commerce payment

What banks should do when confronted with: Zeus, GameOver and other attacks, Preparedness initiatives – part of legal compliance.

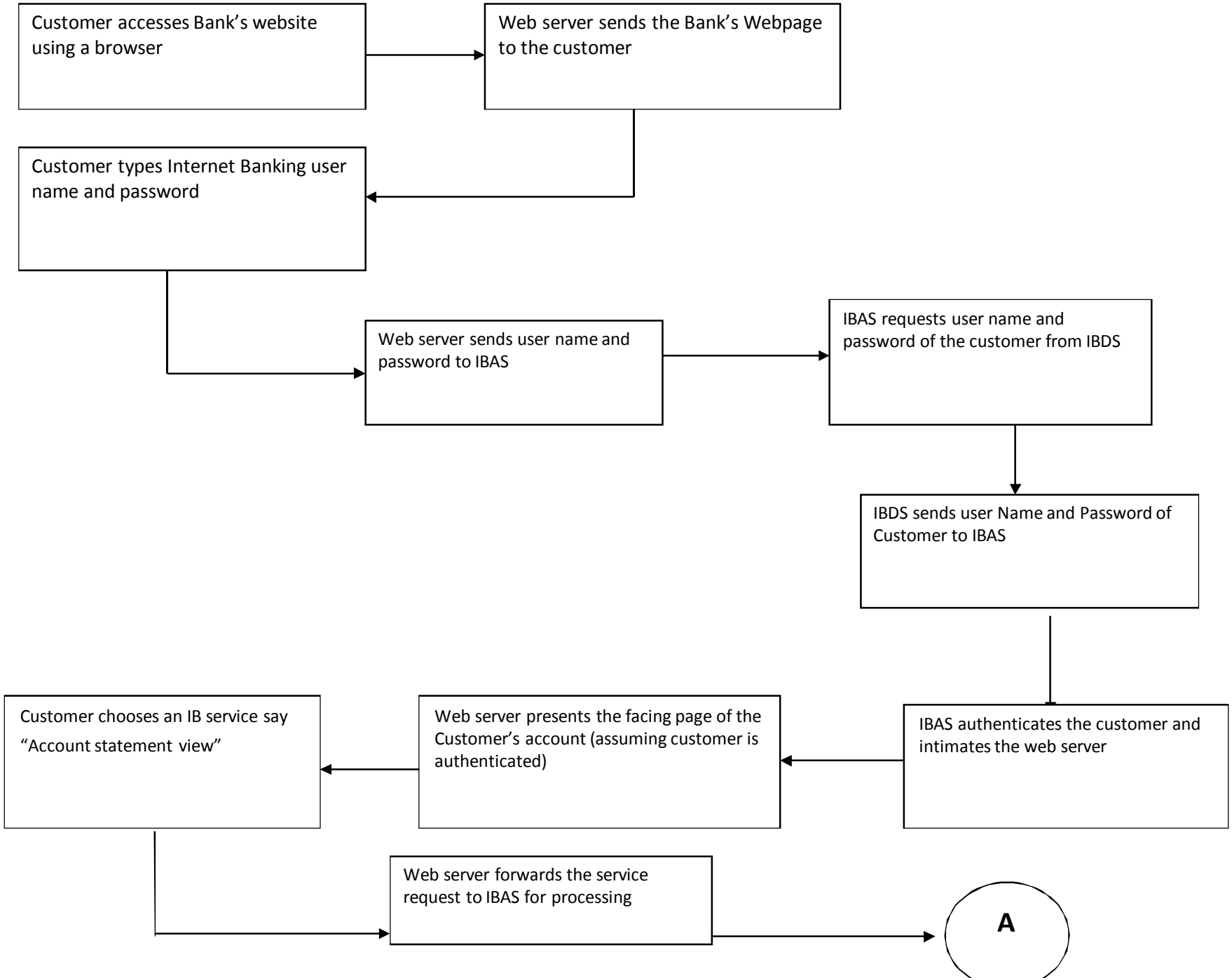
Internet Banking

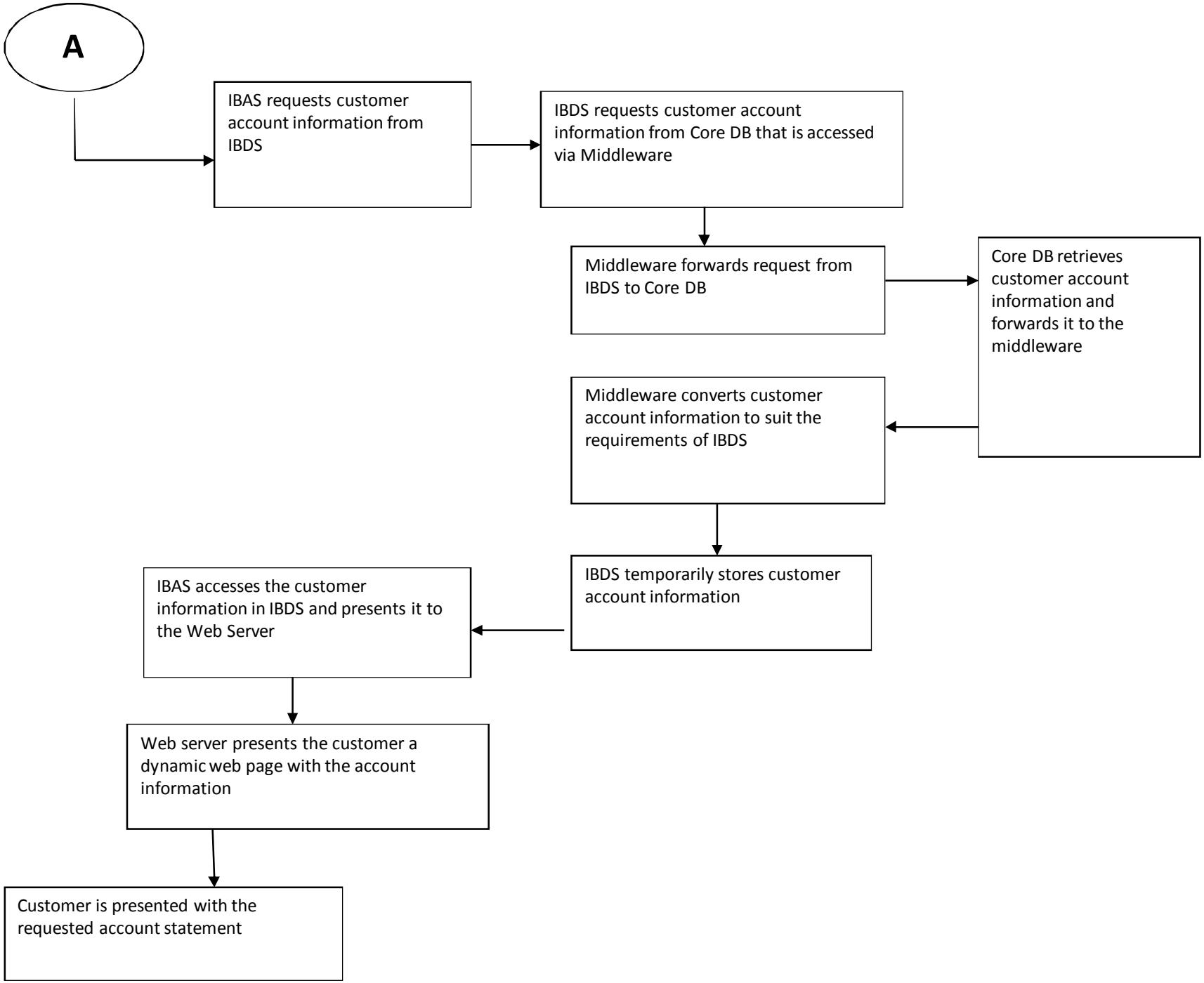
- Banks to guard against “Phishing” sites
- Banks will never require your info to be typed and mailed to them
- Banks do not give any link to other site/s which demand particulars from the users
- Remember the site-names
- Look for site certifications: verisign
- Payment thro’ e-banking:

  Use of CVV in VISA or CVC in Master

Internet Banking - Technology

- Internet Banking involves a CBS process
- Webserver and web-host
- Role of IBApp Server and IBDS
- Meaning and significance of Middleware
- Central Database Server
- The specific service requested – IBAS and IBDS
- Presentation to the customer in a browser
- Dynamic web-page getting refreshed


Customer accesses Bank's website using a browser
Web server sends the Bank's Webpage to the customer
Customer types Internet Banking user name and password
Web server sends user name and password to IBAS
IBAS requests user name and password of the customer from IBDS
IBDS sends user Name and Password of Customer to IBAS
IBAS authenticates the customer and intimates the web server
Web server presents the facing page of the Customer's account (assuming customer is authenticated)
Customer chooses an IB service say "Account statement view"
Web server forwards the service request to IBAS for processing
A


A
IBAS requests customer account information from IBDS
IBDS requests customer account information from Core DB that is accessed via Middleware
Middleware forwards request from IBDS to Core DB
Core DB retrieves customer account information and forwards it to the middleware
Middleware converts customer account information to suit the requirements of IBDS
IBDS temporarily stores customer account information
IBAS accesses the customer information in IBDS and presents it to the Web Server
Web server presents the customer a dynamic web page with the account information
Customer is presented with the requested account statement

Process Flow

- Customer choose his function say statement of account
- Web server send information to IBAS
- IBAS access IBDS for getting data
- IBDS will interact with Central DB server through middleware
- Middleware convert the data to suit the requirement of central DB
- IBDS forward customer data to IBAS which process the request
- Statement of accounts from central DB made available to IBDS
- IBDS will send to IBAS then to web browser
- Web server generate dynamic web pages
- Customer will get their required services.

Internet Banking - Controls & Audit

- User creation – through front-end or customer physically signing the request at the branch?
- User maintenance – id verification, forgot password option, reset requests
- Audit of logs – modification of requests
- Logs at the branch and at the Data Centre level
- Testing and verification of IBAS software
- 2FA in IBAS
- Guard against: vishing, DDoS, Hackers etc

Controls and Security concerns

- Authentication process
- Procedures and steps taken by IBAS and IBDS
- Validation by the server – User authentication
- Security concerns include:
  - Guarding against wrong or fraudulent transfers
  - Privacy and confidentiality of customer accounts
  - Quick complaint redress mechanism
- Controls should be constantly evaluated


CAUTION

Cyber Crimes – Internet Banking

Cyber Crime

Cards, cards and cards everywhere

- Credit Cards
- Debit Cards
- Visa Cards
- Master Cards
- Smart Cards
- RuPay cards
- Other merchant Cards like Diners etc

Credit Cards

Parties to a credit card – the trio

Roles and responsibility of issuing bank

Pre-sales identification of borrower

Responsibilities of merchants

Liabilities of a customer

Take-over of liabilities from other banks

Banking practices –hidden charges

Role of regulators in evolving guidelines

Role of consumer organisations

Debit Cards in e-commerce

- Debit cards different from credit cards
- Bank's role: Accounting &Technological
- Loss of a debit card vs loss of a credit card
- Up-keep and maintenance
- Shop-keeper's responsibilities in both
- ATM Cards – debit to one's account
- Inter-bank debits and reconciliation issues

Payment through PoS terminals

- 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

Security concerns in Card payments

- Merchant's responsibility verify sign, photo
- CCs with PIN used in some countries which the customer enters – Not so far in India
- 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

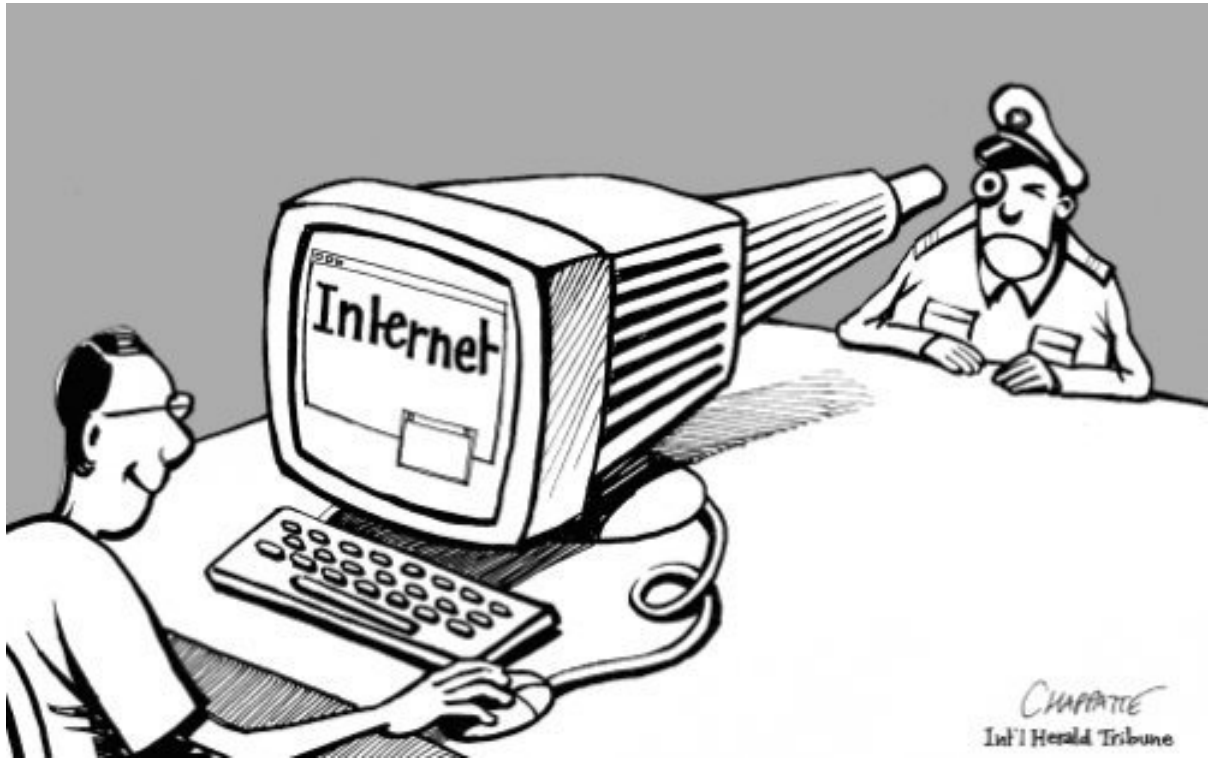
  at the bank's premises

  at the courier office

Is there anything like 100% security?

While on the net, you are always watched!

Software downloads, spyware, malware, adwares..



Cyber Crimes - Cards

- Physical security:

  Theft of cards, Additional security features in cards like grid information, signature verification, photo cards, PIN in addition to swiping at PoS terminal,

- Shopkeepers' responsibility
- Bank's responsibility:
  - Despatch of card and PIN mailer, Handling confiscated or surrendered rejected cards, attending to card-lost and card-misplaced complaints on 24 x 7 basis
  - Security initiatives: OTP, Session PINs, Grid information, PIN for use at PoS

Cyber Crimes - Cards contd

- Users' responsibility –
  - **Never**:
    - give card to anyone
    - write the PIN anywhere
    - allow the card to be out of sight
  - Permit swiping at only one device – the PoS device only
  - Never give back-to-back xerox copy
  - Guard against skimming – always
  - Opt for an additional authentication

Mobile Banking

- Mobile Banking in India –
  road ahead
- Features in Mobile Banking
- Awareness initiatives
- Mobile Device – convergence of all

  A single point gadget

  A single point threat

  Lose the mobile and lose everything?

CBS Data Centre

- Role of Data Centre personnel
- Data Centre and the technology behind it
- Backup and redundancy:
  - Hardware, software, O/s, network, gadget, third party interfaces and backup for everything
- Role functions of system administration
- Role functions of security admnistration

Compliance issues in Banks

- 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

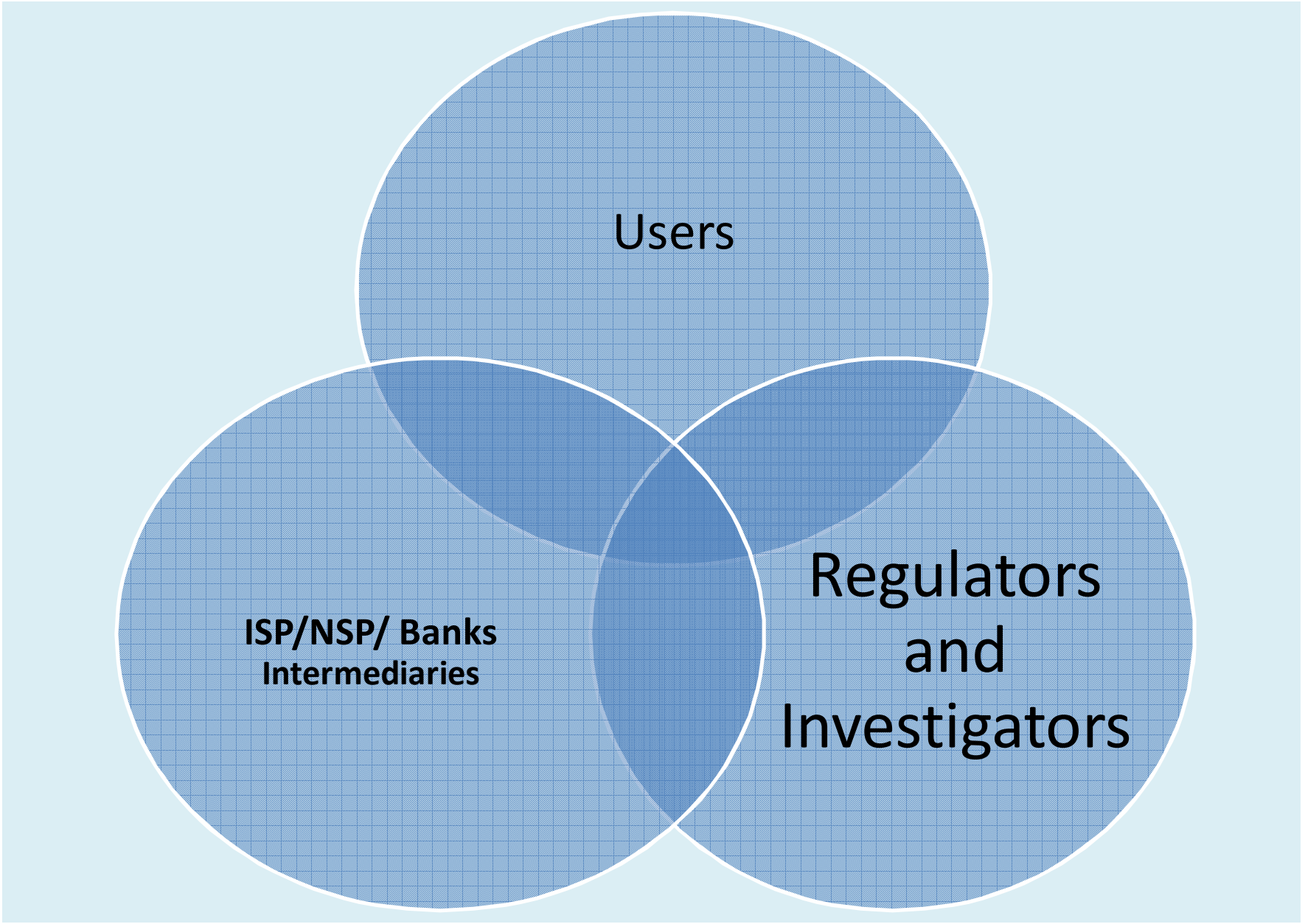
Role of Banks in Cyber Law Compliance

- Information Sharing – Mandatory?
- Data on cyber crimes and victimisation
  - Real data, adverse publicity, cost of security, ease of use vs security of data, image of being tech-savvy
- Most often, the real data does not come out
- Role of bank managements, top management, officers' associations, employees and others
- Role of IBA
- RBI as regulator or facilitator?

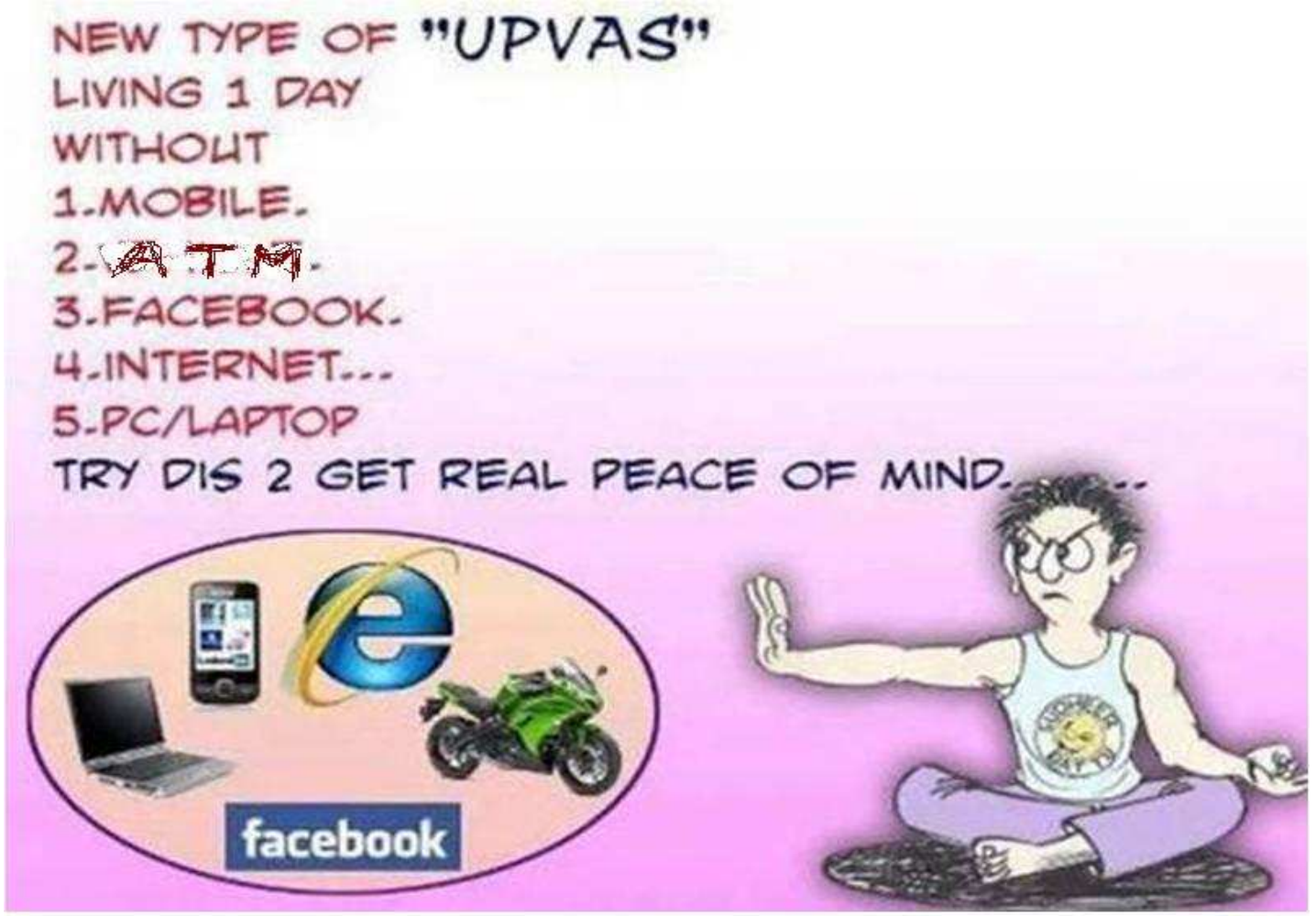
RBI – Regulatory Compliance

- Master Circular dated 1-7-14 on “Frauds” –
  - Cyber crimes included in the general list of frauds
  - Reporting mechanism, amount-wise classification etc
  - Classification based on IPC and related heads
- Circulars on Banking Ombudsman
- RBI’s Annual Reports – Compliance report by banks
- Transparency by banks: Public and Private Sector

Information Security



Banking without technology?



Questions ???

Thank you…..

V. Rajendran
URL : venkrajen.in
venkrajen@yahoo.com
rajcyberlaw@gmail.com
+91-44-22473849; +91-9444073849