# Legal Issues of E Banking

Naavi

9th April 2021

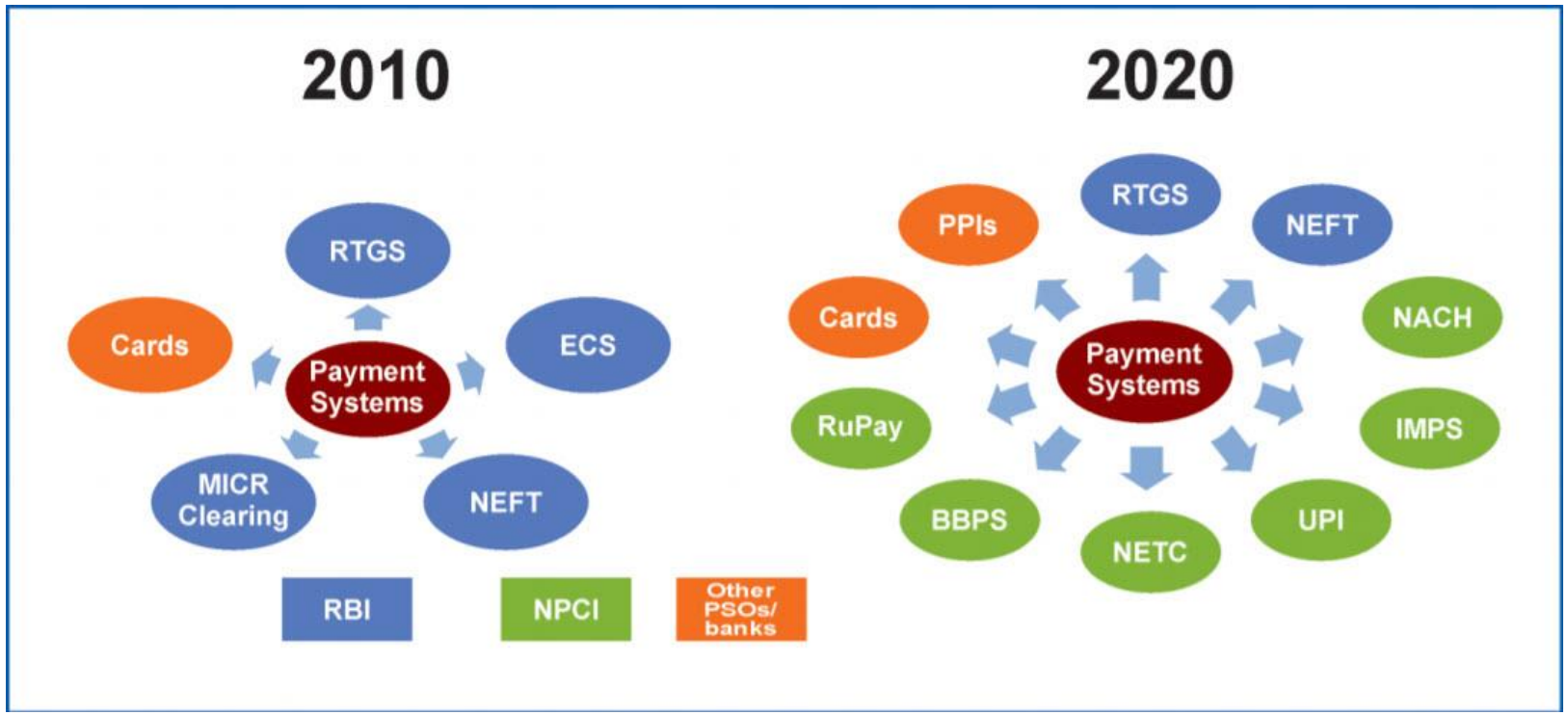
# What distinguishes E Banking?

- Traditional Banking used “Paper” as the means of
  - Recording of transactions
  - Exchange of material instructions between the Banker and Customer
  - Account opening was a contract under Indian Contract Act using paper based offer and acceptance documents
- Interaction with the customer was face to face
  - With the ledger clerk initiating a transaction
  - branch manager who authenticates a transaction
  - the cashier who dispenses cash
    - E Banking uses an electronic document or an electronic device for either record keeping or for interaction

# Evolution of e-Banking

- Human interface continued
  - Bank end computerization introduced
  - Interbranch reconciliation
  - ALPM, Branch network, Core Banking
  - Internet Banking was an add-on channel
    - Now it is the main channel
    - Along with Mobile

# India's Payment Systems



# Legal Definition?

- There is no separate definition.
- The derived definition
  - E Banking means
    - “Banking” with the use of electronic documents. Or
  - *“accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque, draft, order or otherwise using electronic documents in the process”*
    - Use of electronic documents implies use of electronic devices

# Advent of Internet banking

- Originated in 1997-ICICI bank when there was no legal recognition of electronic documents
  - Initially for Viewing of Account transactions
  - Funds transfer within the bank (NEFT)
  - Fund transfer outside the banks (RTGS)
  - Now IMPS
  - Bill payments
    - Virtual Banking scenario, Anywhere, Anytime Banking

# Card Banking

- Storage of Information
  - Magnetic Stripe or Chip
  - Elementary identity particulars or more
    - It is a data storage device or “Media” as per ITA 2008
    - The card swiping device reads the data and transmits the data.
      - It is a “Computer” as per ITA 2008
  - RFID tagged/Near field communication contact less cards
  - EMV standard with Microprocessor Chip

# Social Media/E Mail Banking

- Facebook/Twitter
  - Send a message to the facebook page
  - Send a message to a Twitter account
  - Send payment to an e-mail address
    - Receiving Bank issues a payment authorization with a Pin acceptable at an ATM
- Customer ID is linked to the social media account/E Mail account
- Transmission of instruction is through the Internet

# App based banking

- Bank specific App
  - Linked to a Bank
- Multi bank App (Wallet)
  - Is a Bank in itself.
- Apps that enable peripheral interaction with the core banking system
- Apps that are capable of carrying out full fledged transactions of money transfers in and out.

# New Forms of Banking

- USSD Based Banking
- IVR Banking
- Aadhar Based Banking
- Blockchain based Banking?

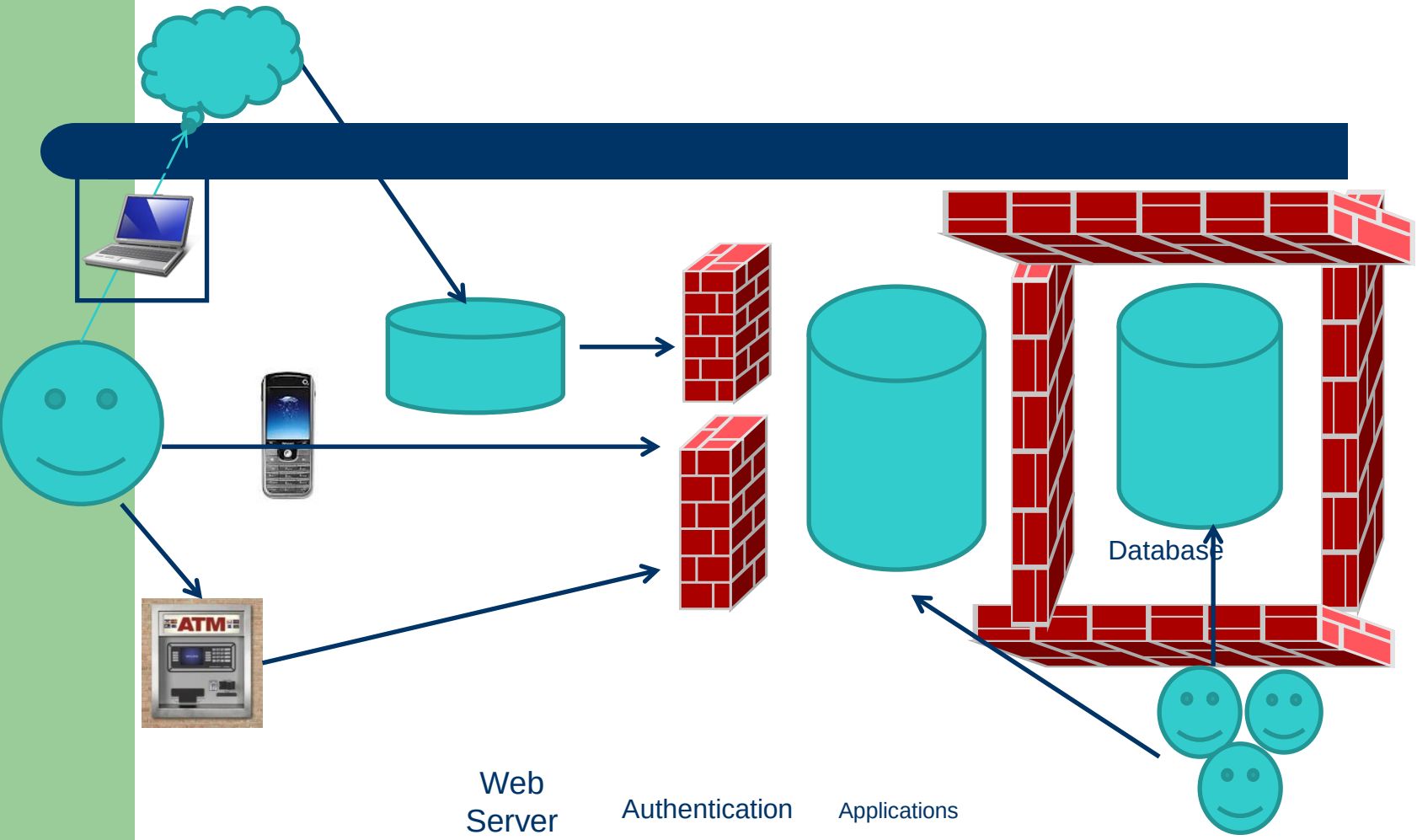
# New Forms of Banking

- UPI
  - Amazon pay, Google pay, Phone pe etc
  - Service provider is the front for marketing
  - Backend is the customer's own Banks
  - NPCI acts as the clearing mechanism for linking UPI ID to the service
  - There is a move to privatize NPCI which also means that the enormous personal data which it may possess passes onto private operators just like CIBIL transferring the data to TransUnion

# Technological Overview

- Electronic Documents held in a data base server
- Transaction applications are hosted in an application server
- Access is through an authentication  gateway or Firewall

# E Banking architecture



# Legal Aspects of E Banking

Naavi

# What is the Applicable Law?

- All laws and regulations applicable to Banking
  - RBI Act, Banker's Book Evidence Act, Banking Regulation Act, Negotiable Instrument Act, Consumer Protection Act, Indian Contract Act
  - Superimposed with the law applicable for use of electronic documents..ITA 2008
  - Payment and Settlement Act 2007
  - Now the upcoming PDPA
- Regulations of RBI from time to time

# What are the legal responsibilities

- Conduct Banking as per Banking law and regulations
  - If not, be responsible for the liabilities that may arise.
- Conduct Banking which is “Secure” from the view point of the customer
  - Besides protecting its own interests

# Responsibilities under ITA 2000/8

- Enter into a valid Banker Customer Contract
  - Application form on paper? Terms on website?
- Enforceability of Click Wrap and Standard form contracts
- Enforceability of undigitally signed contracts and transaction instructions
- Responsibility for following insecure methods of storage, processing, transmission of sensitive personal data, critical banking transaction data, evidence handling
- Responsibility for omissions and commissions of outsource agents

# Responsibilities under PDPA

- Obtain Explicit Consent from customers
- Restrict activities to meet purpose oriented obligations and protect the rights of customers
- Subject to supervision of the DPA

# When Fraud Occurs…

- Root cause could be
  - Criminal activity of an outsider
  - Negligence of the customer
  - Technology  failure
  - Negligence of the Bank
  - Criminal activity of an employee

# Principle of Proximate cause..

- When multiple factors cause a problem,
  - And between multiple  innocent persons
  - he who had an opportunity to prevent last and failed to do so is more responsible than the others
    - The important point to note is that the proximate cause is the nearest cause and not a remote cause.

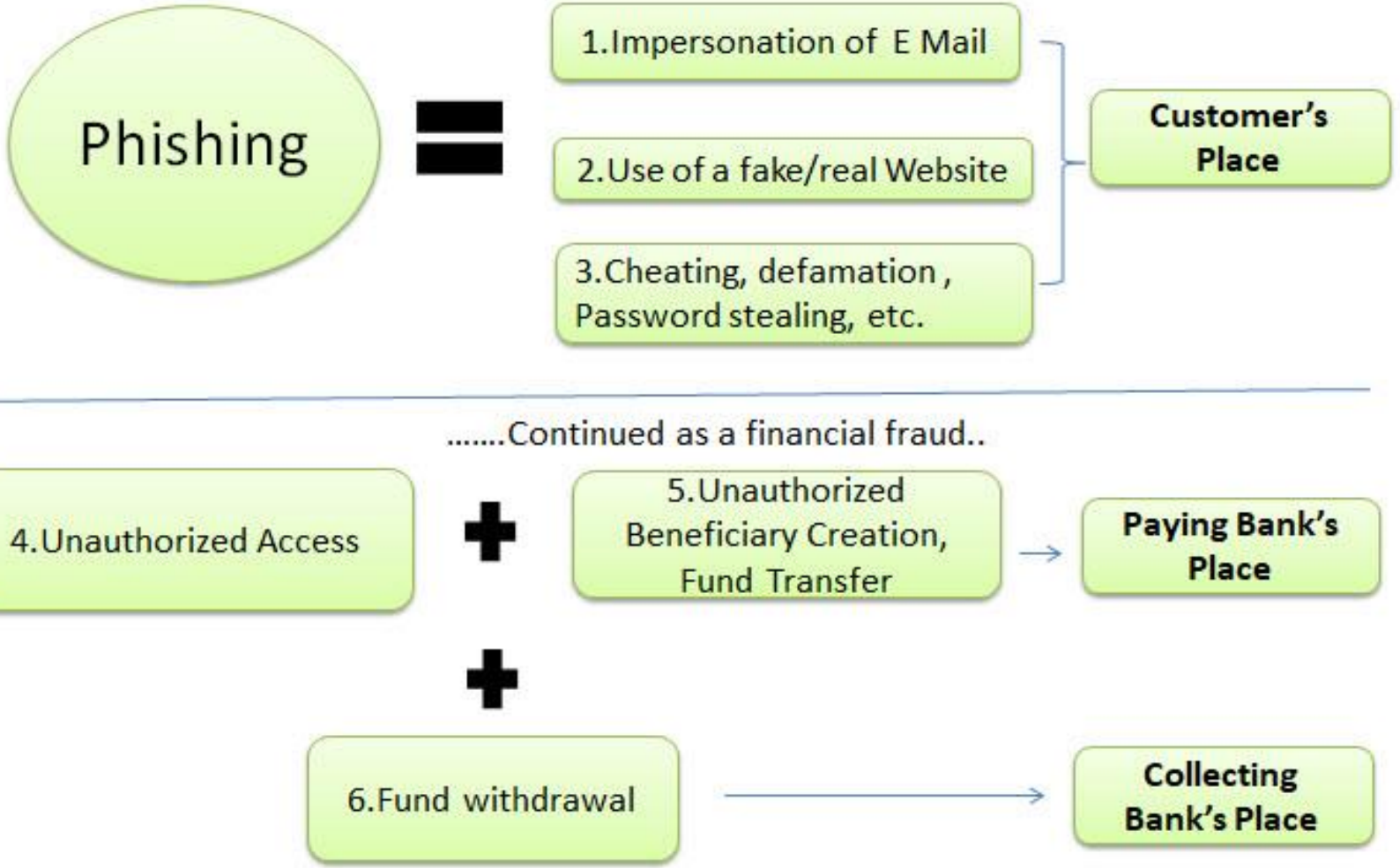
# Vicarious Liability Principle

- Section 85 and Section 79 of ITA 2000/8 as well as IPC recognizes that
  - Liabilities can be borane by persons who have not been beneficiaries or perpetrators of a fraud
    - solely because they had a responsibility for security and were negligent.

# Direct Liability..

- Assistance and Abetment are considered equal to commission of a contravention under Section 43 and Section 84B
  - Passive Assistance can be implied through negligence

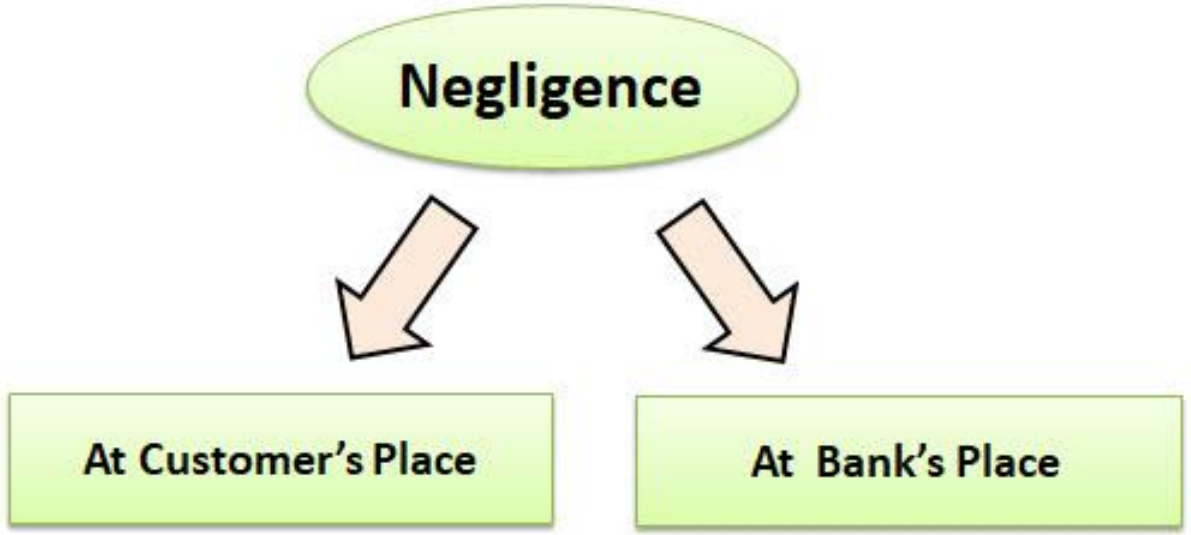
# Techno Legal Perspective of Phishing




Events 1, 2 and 3 are not established to be related to events 4,5 and 6

4

# Anatomy of Negligence




*In a sequence of negligent Acts, it is relevant to check*
*What is the Proximate cause for the loss?*
*Who had the capability to prevent the loss last?*

# Presence of Complicity

## Dimensions of Complicity

| Opening of Account of the Fraudster | During the Commission of the Fraud | After the Fraud |
| --- | --- | --- |
| Failure of KYC (PAN, Sales Tax Registration/ Telephone Bill)<br>Bounced Cheque<br>Rosy projections | Non use of Digital Signatures,<br>Sharing of proceeds,<br>Allowing Cash withdrawal<br>Not reversing the entire fraud proceeds<br>Wait for 1 month e-mail<br>CCTV footage erasure | No Police Complaint,<br>No reply to CrPC Notice,<br>Holding back IP address information |

4

# Bank's Role….Cyber Security

- Reasonable Security Practice under Section 43A
- Due Diligence under Section 79
- Ability to provide assistance to designated authorities under Sections 69.69A,69B, 70B etc
- Ability to preserve evidence under Section 65 and other laws such as IPC

# Bank's Role….Cyber Security

- ISO 27001 or PCI DSS etc are only means to an end and not the end in itself
- Banks Role is to maintain an infrastructure which takes into account all reasonable security measures to prevent losses occurring to its customers and to itself.
  - "Reasonable" is subject to interpretation and can be stretched
    - Principal guideline is the law of the land and includes what RBI mandates

# Follow RBI Guidelines

- Cyber Security Framework of June 2, 2016
  - Continuation of GGWG guidelines of 2011
    - Continuation of the Internet Banking guidelines of 2001

# Follow RBI Guidelines..

- Internet Banking Guidelines 2001
  - Wanted Banks to adopt Cyber Insurance
  - Assume legal risk if digital signatures are not used
- GGWG guidelines of 2011
  - Wanted Banks to mandatorily conduct ITA 2008 compliance exercise
  - Gave a comprehensive structure for information security management including
    - Organizational structure, Outsource agents management, Customer education etc besides technical requirements
      - How much of these guidelines we have complied with?

# Follow RBI Guidelines

- Cyber Security Framework of June 2, 2016
  - Required a Gap analysis to be completed by July 31, 2016
  - Required compliance by September 30, 2016

# Cyber Security Framework

- 24 baseline controls indicated
- Cyber SOC mandated
  - To include monitoring of zero day vulnerabilities
- Cyber Incidents to be Reported

# Salient Features of the CSF-2016

- Board's responsibility increased
  - Board to be approved of the Gap report to be submitted to RBI (by July 31, 2016)
  - Board to approve  Cyber Security Policy (by Sept 30, 2016)
- Continuous Surveillance indicated
  - Not "Audit" approach…good for the  day and time the auditor signs off.
  - Requires setting up of an SOC either on its own or in consortium

# Salient Features of the CSF-2016

- Banks to assume responsibilities for data with its sub contractors
  - suitable systems and processes across the data/information lifecycle need to be put in place by banks.

# Salient Features of the CSF-2016

- Cyber Crisis Management Plan to be developed
  - Wider than the DRP/BCP
  - Should incorporate CERT IN and IDRBT suggestions
- CCMP Should address the following four aspects:
  - (i) Detection
  - (ii) Response
  - (iii) Recovery and
  - (iv) Containment

# Salient Features of the CSF-2016

- Zero day vulnerabilities/attacks  to be taken note of
  - Mere patching of vulnerabilities insufficient
  - Requires maintenance of Honeypots  either on own or on consortium basis
- Ransomware/Cryptoware defense to be built
- Threats such as
  - business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.
    - to be guarded against

# Salient Features of the CSF-2016

- Cyber Security Preparedness indicators to be developed and
- audits to be conducted against such measurable parameters
- Summary level information to be reported to RBI
- CISO Forum to be used for sharing information

# Key Measures

- Phishing
  - Identify and Bring down Phishing  websites ASAP
  - Use legally acceptable means of access and not commercially convenient methods
    - Digital Signatures instead of passwords or biometrics
  - Don’t Rely entirely on 2F authentication
    - Neither legally sound nor technically secure

# Website/App malware

- Watch every page of the Bank’s website in real time  for injection of malware either through modified content or advertisements
- Secure Apps against fake apps and security vulnerabilities

# ATM Watch

- ATMs are extended Bank premises
  - Includes  ATMs managed by other Banks or agents
  - A Customer may consider his  Bank as responsible for any loss arising out of his visit to the ATM.
  - Malfunctioning CCTVs, guards or installation of “card skimmers”, “lebanese loop”, “key blocking matchsticks”, etc are the responsibilities of the Bank

# Remedies to Bank fraud victims

- Limited Liability Claim
- Ombudsman when there is violation of RBI guidelines
- Consumer Courts when there is service deficiency
- Adjudication when there is a contravention of ITA 2000

# Limited Liability for E Banking Frauds

July 6 2017

# Essential Features of Limited Liability

- When a loss occurs on account of an E Banking Fraud, the fraud would be classified as
  - **A: Zero Liability Incident**
  - **B: Limited Liability Incident**

# Zero Liability Incident

- The **“Zero Liability Incident”** is one in which the Customer shall not be liable and the Banks should reverse the amount lost within 10 days.
  - This is applicable when the security architecture and systems of the bank for electronic banking transactions are not able to protect the customer in case of
  - **a) Fraud or Negligence on the part of the Bank**
    - irrespective of whether the loss was reported by the customer or not
  - **b) Third party breach**
    - where the fault lies neither with the Bank nor with the customer and
    - the **customer notifies the Bank within three working days** of receiving communication from the bank regarding the unauthorized transaction
  - **c) Involving Negligence of the customer**
    - such as sharing of payment credentials
    - **after the customer reports** the unauthorized transaction to the Bank

# Limited Liability Incident

- The **“Limited Liability Incident”** is one where the customer has to bear the loss to a limited extent and would cover the following cases.
  - a) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor the Customer and
    - the customer notifies the Bank of the unauthorized nature of the transaction between 4 to 7 days
    - -the liability of the customer is limited to the lower of the transaction value or
      - Rs 5000/- (BSBD accounts)
      - Rs 10000 for accounts with average balance of upto Rs 25 lakhs and Credit card wuth limit upto Rs 5 lakhs, or
      - Rs 25000 for others

# Policy for settlement

- Where the customer notifies the Bank after 7 days, the liability will be determined as per the Bank's approved policy.
- **Banks shall provide the details** of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts.
- Banks shall also display their approved policy in public domain for wider dissemination. The **existing customers must also be individually informed** about the bank's policy.
  - It is reasonable to expect that the liability will be still limited and cannot be 100% of the transaction value

# Credit within 10 days

- Bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account **within 10 working days** from the date of such notification by the customer (without waiting for settlement of insurance claim, if any).
- **Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.**
- The credit shall be value dated to be as of the date of the unauthorised transaction.
- Further the complaint shall be resolved by the Bank within 90 days failing which the Band should reimburse the amount to the customer ensuring that there is no interest loss to the customer.

# Burden of Proof

- The burden of proving customer liability in case of unauthorised electronic banking transactions will lie on the bank.

# Security Procedures to be adopted

- The circular mandates that the systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions.
- To achieve this, banks must put in place:
  - appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
  - robust and dynamic fraud detection and prevention mechanism;
  - mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events;
  - appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and
  - a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud

# Mobile alert

- It is the Bank's responsibility to ensure that a mobile alert is provided for "All Debits".
- When an alert comes in, the customer needs to check and if the transaction is not authorized, he should immediately report to the Bank for which Bank should publish contact information and provide for a "Reply" to the message.
- If the customer is missing any alert, he should record it by informing the Bank and keeping record of such reports.
- If the customer is going abroad where he may miss the alert, he should ensure that the account is suitably locked or alternate arrangements are made by limiting the transaction limits.

# Mobile alert

- Whenever the Bank receives any instruction from the customer, the banks should match the location of the transaction with the known location of the customer (eg: he is abroad or he is in the village when the transaction is reported from elsewhere etc).
- Even the OTP is answered from a mobile whose location is easily available to the Bank and if they are not having systems to monitor these, it should be considered as “Inadequate security” and challenged.

# Mobile Alert

- We suggest that Banks introduce a system by which the transactions should have a mandatory gap of at least 5 minutes between two successive transactions to avoid such frauds besides an option to the customer to switch off the transactions any time he wants.
- Customers should be able to switch on the transactions at will and switch it off immediately after the transaction.
- For this purpose the alert should have an automatic option to switch off for a stated period like we put our WhatsApp on “mute” from time to time

# Similar Guidelines Extended

- Cooperative Banks
  - December 14, 2017
  - Under similar terms
- Prepaid Instruments on January 4, 2019
- Banking Ombudsman scheme
  - also extended to digital payments on January 31, 2019
    - Has to follow the Limited Liability system

# Judicial View

- The liability of the Banks in case of “Lack of Due Diligence” established in S.Umashankar Vs ICICI Bank
  - Adjudicator of Tamil Nadu in 2010
  - Upheld by TDSAT in 2019
- Kerala High Court in PV George Vs SBI
  - 9th January 2019
    - Not answering the SMS alert cannot absolve the Bank of liability.
      - Limited liability fortified beyond what was stated in the circular

# Data Protection Related

- Look at PDPSI as a framework to supplement ISO 27001
- Use the DPERT service of FDPPI

# Thank You

**For More Information**:

Query using the Android App: **Cyber Law Guru**

Available for free download in Google Playstore


Naavi@vsnl.com
www.naavi.org
+919343554943