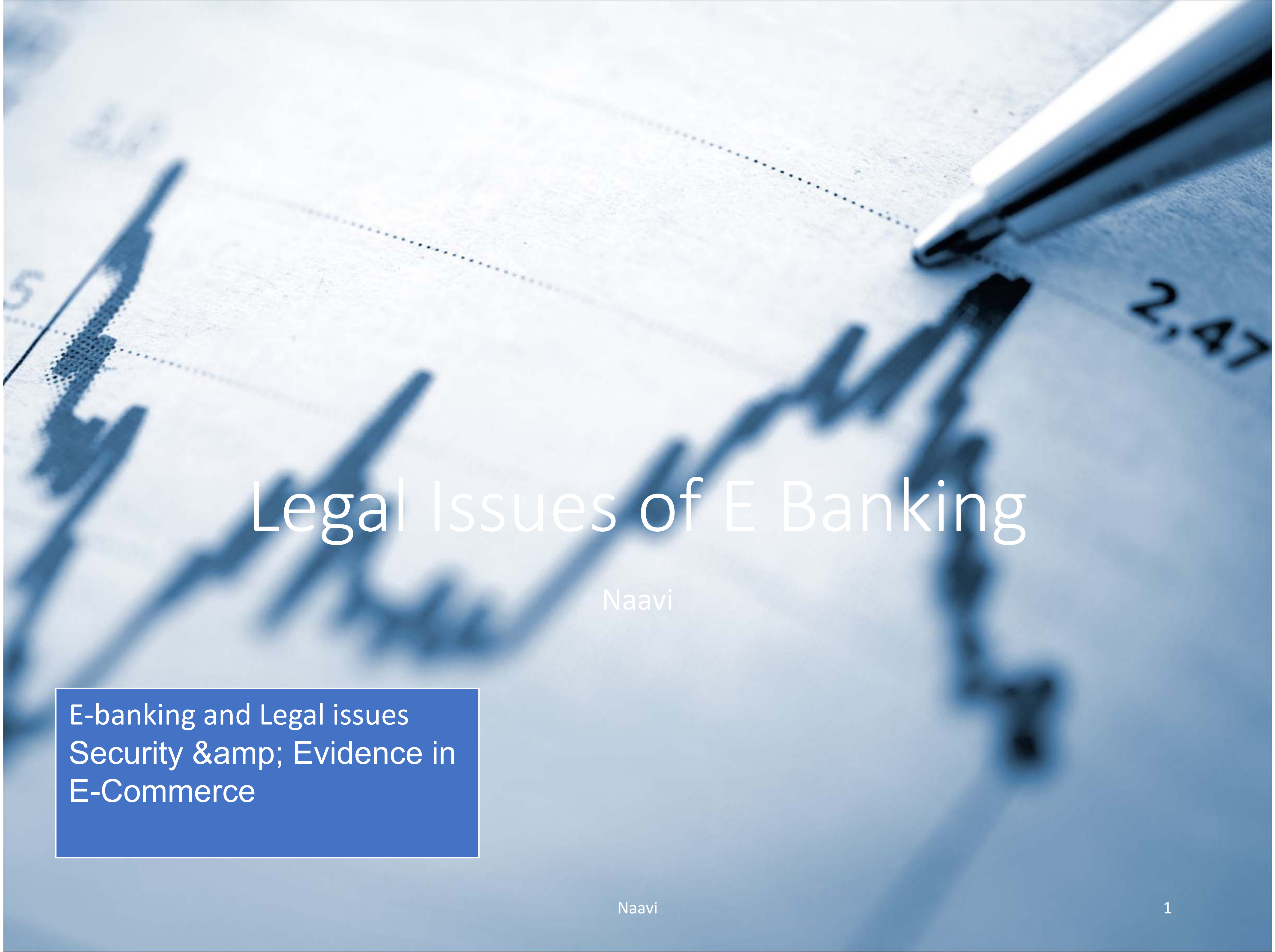
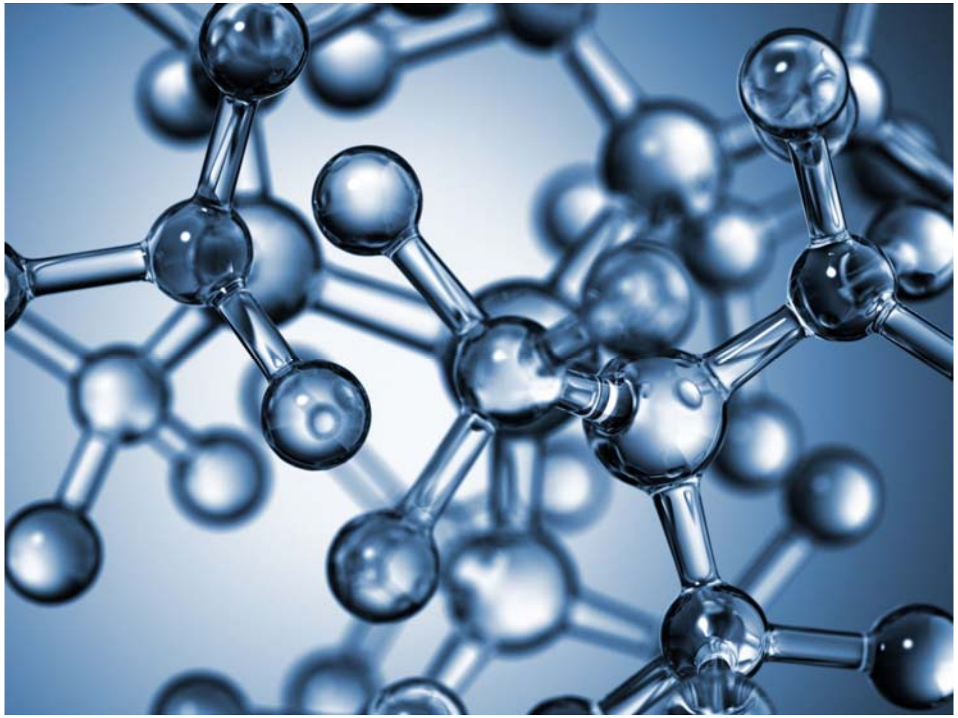


Legal Issues of E Banking

Naavi

E-banking and Legal issues
Security & Evidence in E-Commerce



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/Officer 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 between the customer and the Bank and internally from one Bank employee to another

Naavi

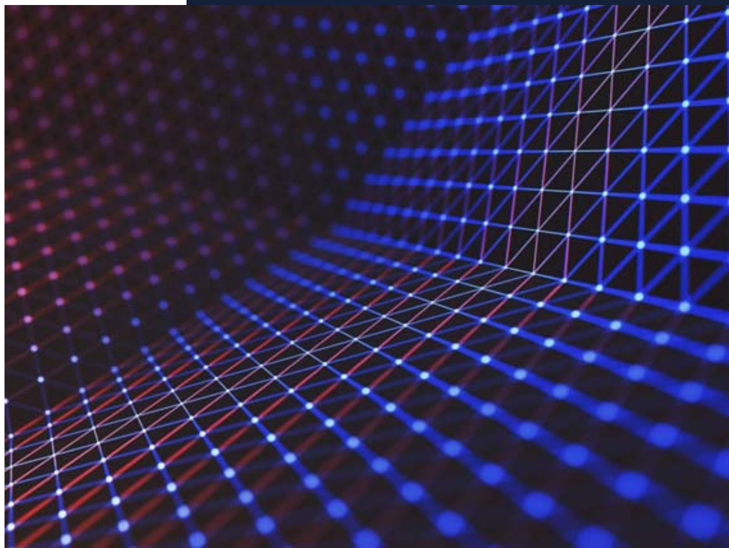
Evolution of e-Banking

- 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
  - IT was a tool of the Bank employee. Customer had no direct responsibility

Evolution of e-Banking

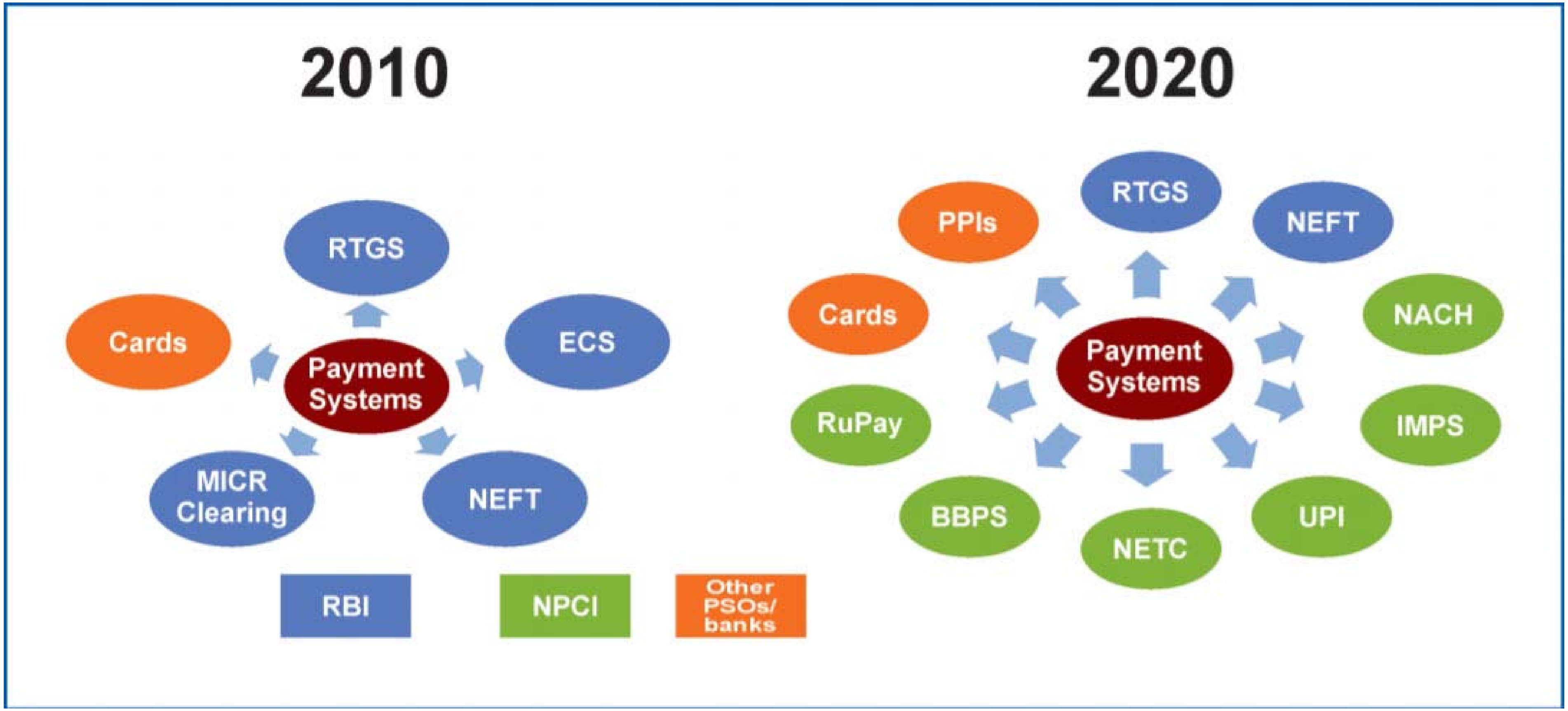
Inter Branch transactions

- Carried on earlier through Clearing houses with representatives of each Bank exchanging cheques on each other
  - Provisionally settling the payments through the RBI (Clearing Bank) account
  - Returning instruments in the return clearing if it is not passed by the back end branch.
    - Wrongful dishonour, Consequences, NI act, Section 138 liability etc were part of this system



In the e-Banking scenario, Inter Bank reconciliation systems have changed

India's Payment Systems

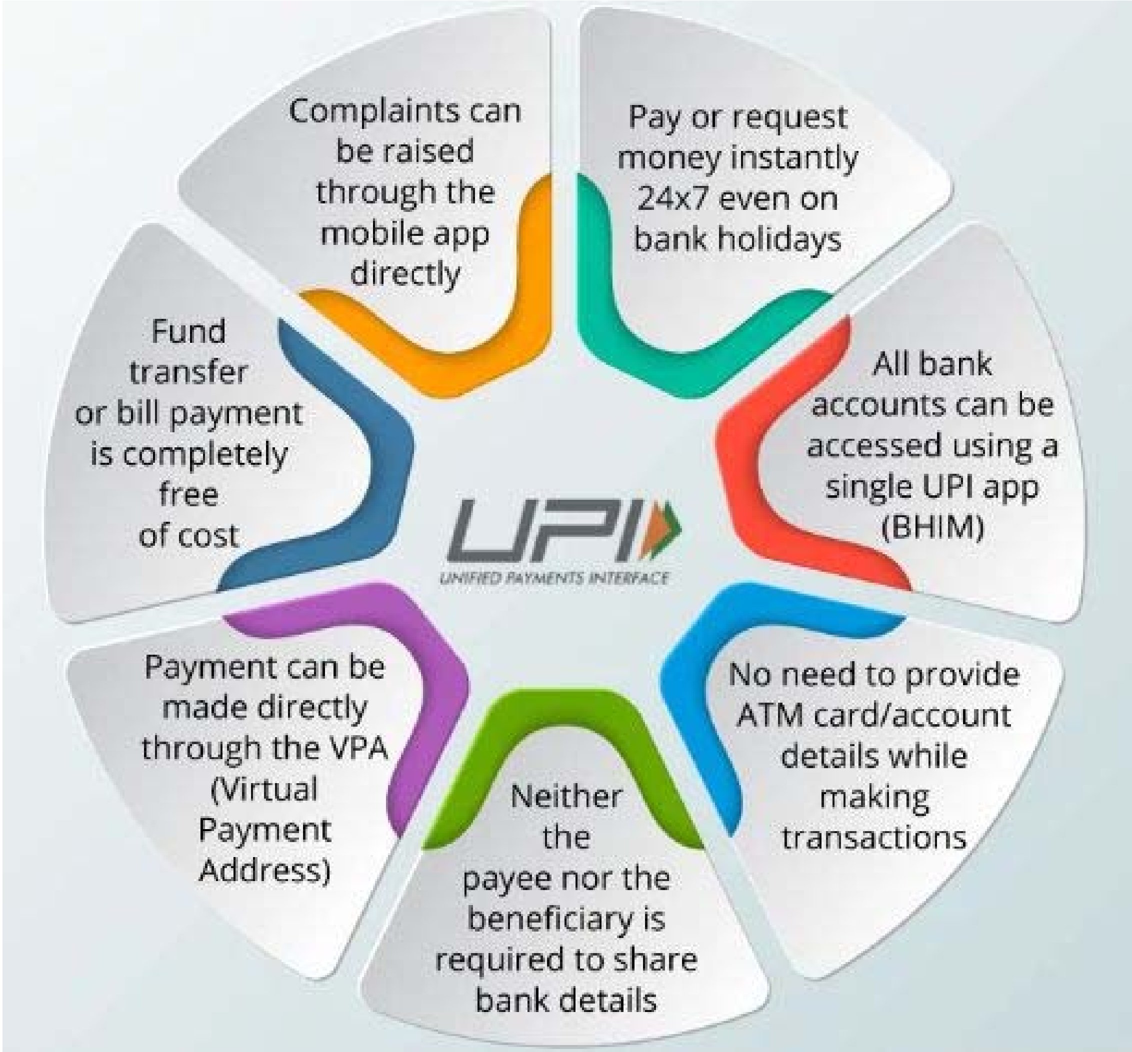


UPI System

- Real-time payment system that was launched by the National Payments Corporation of India (NPCI) in 2016
- Enables instant money transfers between bank accounts through a mobile device
- More than 382 banks that have enabled UPI payments, and the system has processed over 8.03 billion transactions in Jan 23, with a total value of over INR 12.98 trillion

UPI System

- Phone Pe and Google Pay together account for 82% of UPI transactions by volume (47% and 35% respectively) and 84% by value (49% and 35% respectively)



Naavi

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

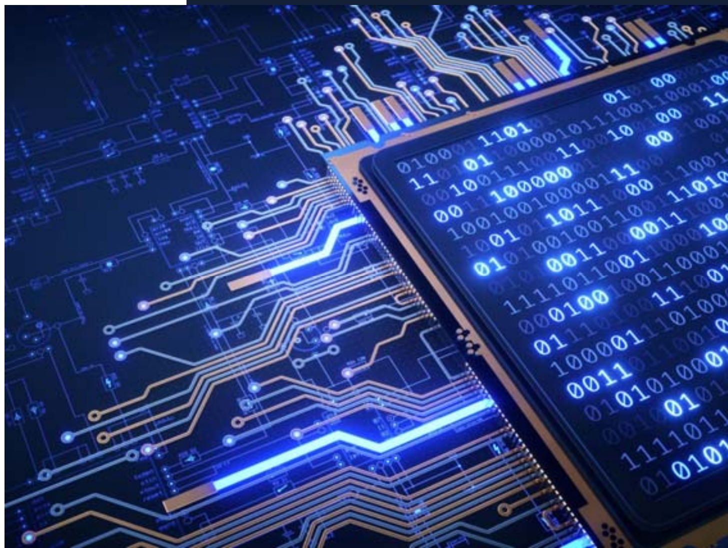
Naavi

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

Naavi

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?

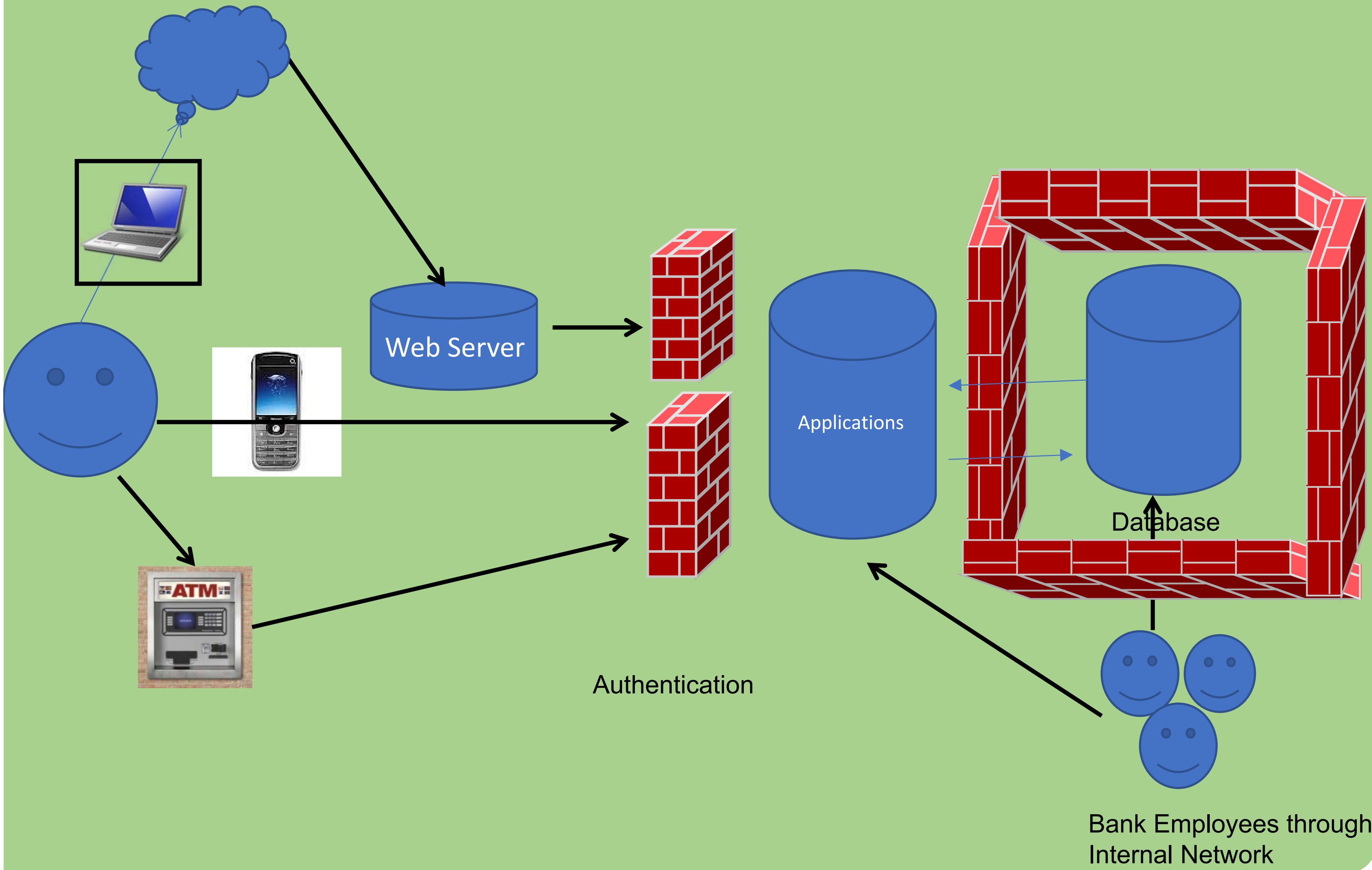
New Forms of Banking

- 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
  - Data can be accessed both by customers as well as internal employees

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 DPDPB

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

Naavi

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

Naavi

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.

Naavi

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

Phishing =

1.Impersonation of E Mail

2.Use of a fake/real Website

3.Cheating, defamation , Password stealing, etc.

→ Customer's Place

.......Continued as a financial fraud..

4.Unauthorized Access + 5.Unauthorized Beneficiary Creation, Fund Transfer → Paying Bank's Place

+

6.Fund withdrawal → Collecting Bank's Place

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

Anatomy of Negligence

Negligence

At Customer's Place

At Bank's Place

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

Failure of KYC (PAN, Sales Tax Registration/ Telephone Bill)
Bounced Cheque
Rosy projections

During the Commission of the Fraud

Non use of Digital Signatures,
Sharing of proceeds,
Allowing Cash withdrawal
Not reversing the entire fraud proceeds
Wait for 1 month e-mail
CCTV footage erasure

After the Fraud

No Police Complaint,
No reply to CrPC Notice,
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?

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

Naavi

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

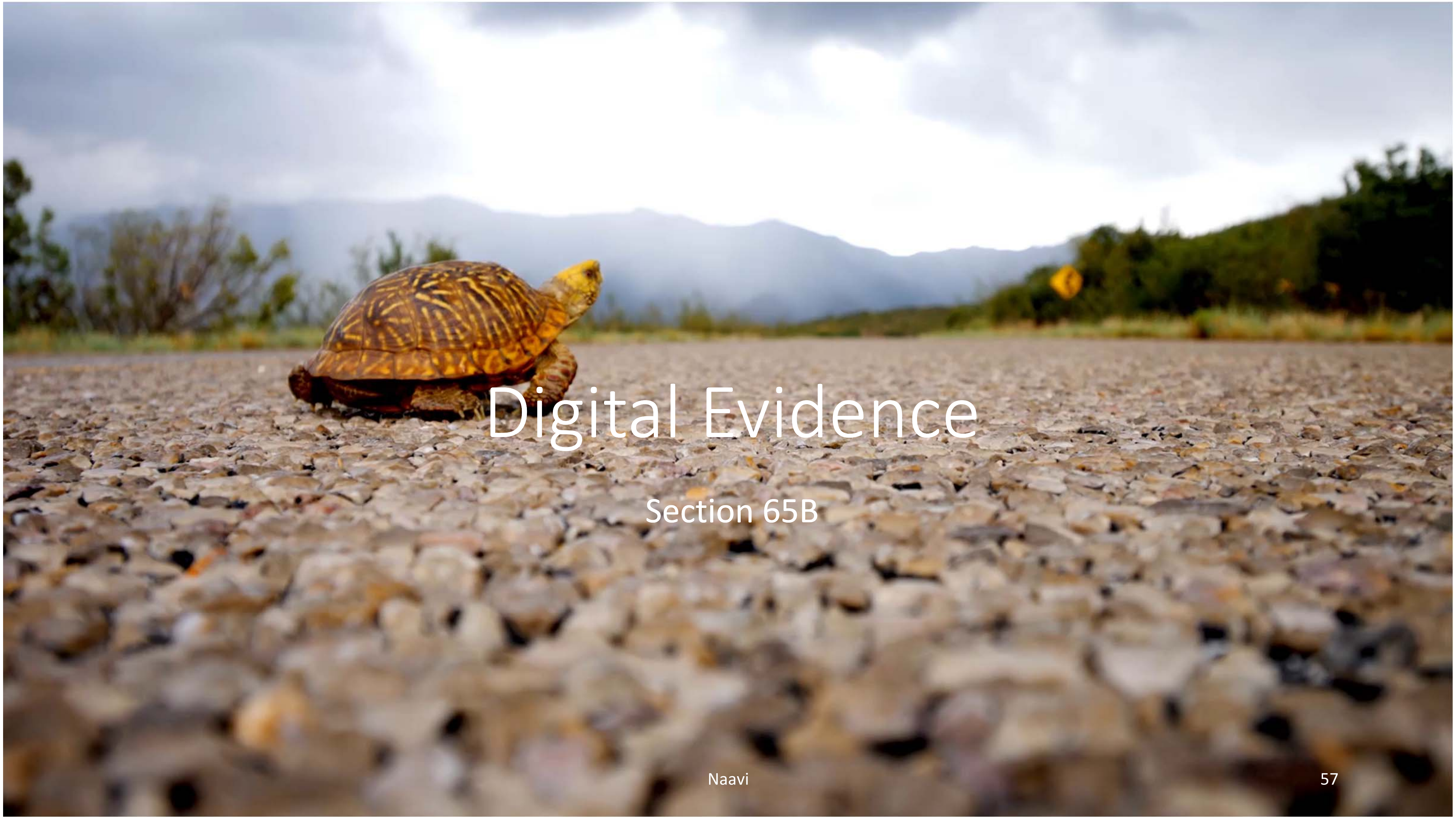
- Cooperative Banks
  - December 14, 2017
  - Under similar terms
- Prepaid Instruments on January 4, 2019
- Banking Ombudsman scheme
  - also extended to digital payments on January 31, 2019
    - Has to follow the Limited Liability system

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

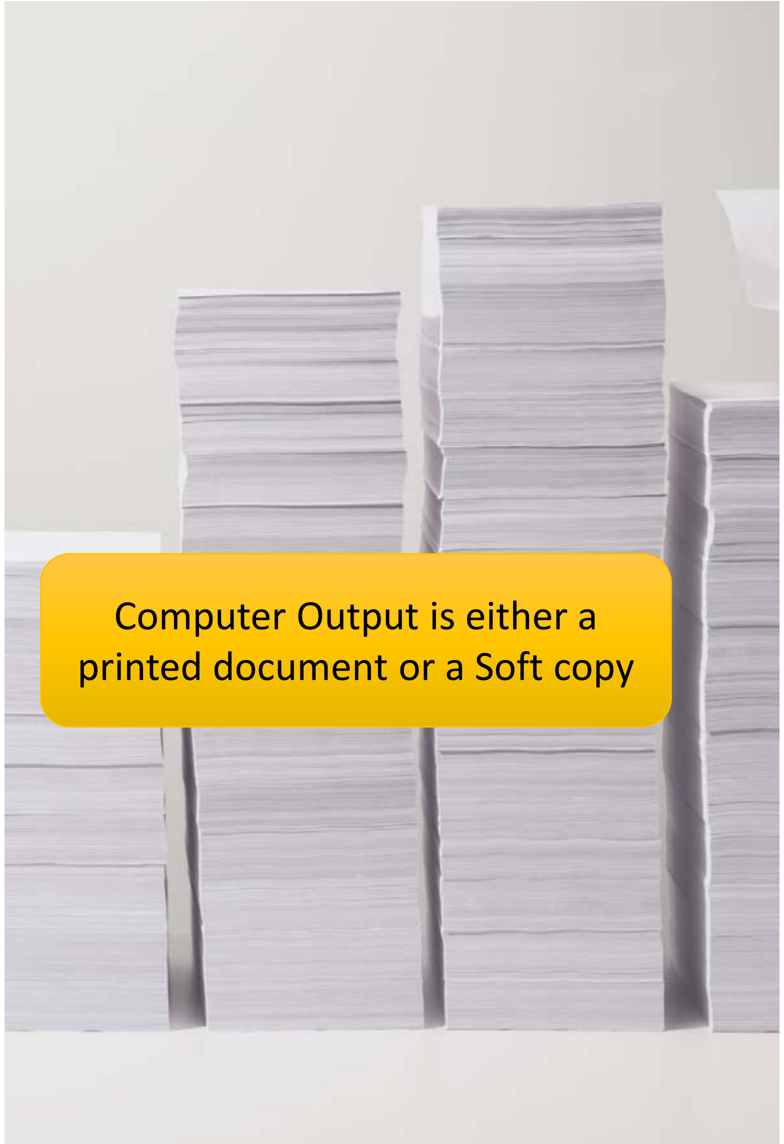
Data Protection Related

- Look at PDPSI as a framework to supplement ISO 27001



Digital Evidence

Section 65B



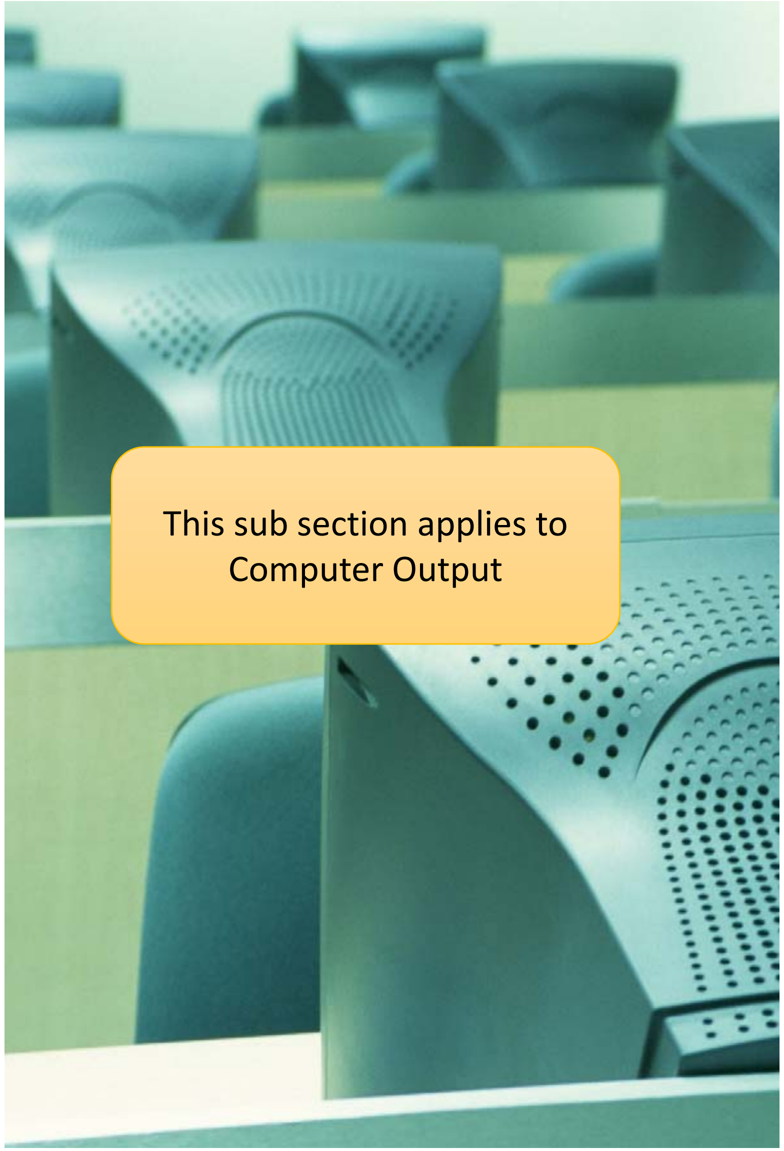
65B. Admissibility of electronic records.-

- (1) Notwithstanding anything contained in this Act,
  - any information contained in an **electronic record**
  - which is **printed on a paper**,
  - **stored, recorded or copied** in optical or magnetic media produced by a computer
  - **<u>(hereinafter referred to as the computer output</u>**)
    - shall be deemed to be **also a document**, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and
      - shall be admissible in any proceedings, **without further proof or production of the original,**
      - as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

65B. Admissibility of electronic records.- conditions

This sub section applies to Computer Output

- (2) The conditions referred to in sub-section (1) **in respect of a computer output** shall be the following, namely:—
  - (a) the computer output containing the information **was produced** by the computer **during the period** over which the computer was used regularly to store or process information for the purposes of **any activities** regularly carried on over that **period** by the **person having lawful control over the use of the computer;**
  - (b) during the said period, information **of the kind** contained in the electronic record or of the kind **from which the information so contained is derived** was regularly fed into the computer **in the ordinary course of the said activities**;
  - (c) throughout the material part of the **said period**, the computer was **operating properly** or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
  - (d) the information contained in the electronic record **reproduces** or is derived from such information fed into the computer in the ordinary course of the said activities.



65B. Admissibility of electronic records.-Multiple Computers

- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of **sub-section (2**) was regularly performed by computers, whether—
  - (a) by a combination of computers operating over that period; or
  - (b) by different computers operating in succession over that period; or
  - (c) by different combinations of computers operating in succession over that period; or
  - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

65B. Admissibility of electronic records.-certification

This sub section applies to Computer Output

(4) In any proceedings where it is desired to give a statement in evidence by virtue of **this section**, a certificate doing any of the following things, that is to say,—

- (a) **identifying the electronic record** containing the statement and describing the manner in which it was produced;
- (b) giving such **particulars of any device involved** in the production of that electronic record as may be appropriate for the purpose of showing that the **electronic record** was produced by a computer;
- (c) dealing with any of the matters to which the conditions mentioned in **sub-section (2)** relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the **relevant device** or the management of the relevant activities (whichever is appropriate)

- shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

65B. Admissibility of electronic records.-certification

(5) For the purposes of this section,—

- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
- (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
- (c) a **computer output** shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

This sub section applies to Computer Output

Cases on Section 65B

First use of Sec 65B

- State of Tamil Nadu Vs Suhas Katti- AMM Court Chennai (2004): 26th October 2004
  - Object of crime was a defamatory message in yahoo group
    - ..considered obscene..contained an impersonated name at the end of the message
    - Conviction was under Section 67 of ITA 2000 along with Section 469 (forgery for harming reputation) and 509 (insulting the modesty of woman)

First use of Sec 65B

- A print out of the copy of the message as seen on the yahoo server was produced by Naavi with Section 65B declarations (Certificate dt 18/2/2004)
  - Original not produced
  - Naavi was not a Government servant
  - Naavi was not the victim.. Was a third party
- Naavi was examined as an “Expert”
  - Court accepted the evidence and convicted the accused for a sentence of 2+2+1 years.
  - Session Courts on appeal upheld the conviction but reduced the sentence

Trisha Defamation Complaint in AMM-2004

- Police had produced CDs seized from a news paper office
- Court could play the CDs and accept it as evidence
  - Chose to call a third party private expert (Naavi) to view the CDs in the chamber, take print outs and certify under Section 65B so that it could be taken for further evidence

Afsan Guru Verdict

- Afzan Guru case, (Navjot Sandhu @Afzan Guru judgement dated 4/8/2005)
- Supreme Court accepted CDs of call records without Section 65B certificate because the persons who could have provided the certificate were also providing oral evidence

Basheer Judgement

- Anvar P.V. Vs P.K.Basheer and others (Supreme Court of India Appeal No 4228 of 2012) …September 18,2014
- Over turned the Afsan Guru judgement and held
  - Section 65B certificate is mandatory for admissibility of any electronic evidence
  - Oral evidence in respect of an electronic document is not acceptable.
  - Admissibility is different from accepting genuinity
  - Section 65B is relevant at the stage of admissibility. Defence can question its genuinity during the trial

Basheer Judgement

- Construction by plaintiff, destruction by defendant.
  - Construction by pleadings, proof by evidence;
  - proof only by relevant and admissible evidence
- What is the nature and manner of admission of electronic records, is one of the principal issues arising for consideration in this appeal
- Genuineness, veracity or reliability of the evidence is seen by the court only after the stage of relevancy and admissibility.
  - These are some of the first principles of evidence.

Retrospective Effect of Basheer Judgement

- **Sonu vs Amar**
  - A convict made an appeal that the conviction had to be set aside since the electronic evidence used was not Section 65B certified
    - Supreme Court held that though the Basheer judgement would be applicable retrospectively, the appeal has to be rejected the appeal that it is not practical to re-open previous convicted cases

Shafhi Mohammad Judgement

- The order dated 30th January 2018 by a two member judge was examining the procedure to be adopted by the Police in videographing the crime scenes.
  - A question was raised that it would be inconvenient to provide Section 65B certificate since the device was in the possession of a third party and not with the police.
  - The order sought to over rule the three member judgement of Basheer Case

Shafhi Mohammad Judgement

- The order stated in "Clarification" of the Basheer judgement that
  - *"The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when*
  - *such electronic evidence is produced by person who is in a position to produce such certificate **being in control of the said device** and not of the opposite party."*

Shafhi Mohammad Judgement

- The order also stated in complete contradiction of the Basheer judgement that
  - "In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded.
  - In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving,"

Shafhi Mohammad Judgement

- The Order is erroneous and
- If applied,
  - Section 65B certificate would not be required for any Facebook, Twitter or Gmail or web document.
  - It would be required only in cases where the person is in possession of the device and if so, the provision is redundant since the original device itself can be brought before the Court
  - It will enable fraudulent documents to be produced at trial stage causing unimaginable problems to honest citizens since onus of proving the document produced as not genuine shifts to the defendant.

Arjun Pandit Rao Vs Kailash Kushanrao-14th July 2020

- Election Commission produced some CDs regarding video recording on filing of nominations but refused to submit Section 65B certificate
- Court held
  - the judgment in Shafhi Mohammad (supra) states the law incorrectly
  - the major premise of Shafhi Mohammad (supra) that such certificate cannot be secured by persons who are not in possession of an electronic device is wholly incorrect.

Thank You …Discussions

naavi@naavi.org

www.naavi.org

+919343554943