LEGAL CHALLENGES IN REGULATING ONLINE AND MOBILE BANKING SECURITY: CYBERSECURITY AND CUSTOMER TRUST

Michelle Julka, Xavier Law School, XIM University

ABSTRACT

Banking holds a significant position in any country's economy. Information Technology has become an indispensable part of today's banking system, which can be attributed to the liberalisation of the economy back in 1992, which increased the competition in every economic sphere globally. Mobile and Internet Banking is a practice that almost everyone is familiar with in today's technologically sophisticated world, especially via private applications such as Paytm, Google Pay, etc. These online banking services benefit the economy and customers. They also help banks reduce customer service costs and the quantity and costs of employees. The downsides to online banking include data phishing scams, security breaches, fraud and hacking, etc.

This submission analyses the legal position of Mobile and Internet Banking in India. It further delves into the RBI guidelines for online and mobile banking, various legislations, and applicable rules dealing with the issues of cyber security and customer trust. The legal, technical, regulatory, and security-based challenges faced along with customers' liability in online banking are also discussed in greater detail in consonance with the guidelines issued by the Central Bank of India.

Keywords: Internet banking, Mobile Banking, Legal Challenges, "Reserve Bank of India Guidelines", "IT Act 2000" [1].

[1] "Information Technology Act, 2000"

INTRODUCTION

In today's day and age where society is technologically so sophisticated, mobile and online banking has become a day-to-day activity. Further, this activity is not just restricted to the country's upper echelons but has appealed to even citizens from lower and middle economic backgrounds. Over the years, online and mobile banking has taken such a prominent place in individuals' lives that even going to the bank has become relatively redundant.

Mobile and Internet banking is on the rise not just in India but globally as well. Both these forms of banking have caused a digital revolution in our country, one which will only make its grip stronger on the generations to come. Soon, the possibility of going to banks may come across as a redundant thought.

"Section 5(b) of the Banking Regulation Act, 1949 states: "banking" means the 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." [2] Thus, online or mobile banking is deemed to be included under banking's definition in the "Banking Regulation Act." [3]

"73 percent of respondents globally use online banking at least once a month, compared to 59 percent who use mobile banking apps. Moreover, it revealed no generational differences in how frequently online banking is used—baby boomers use online banking just as often as tech-savvy millennials." [4]

"Between January and April 2024, Indian citizens suffered losses exceeding Rs 1,750 crore due to cybercriminal activities. This was reported through over 740,000 complaints lodged on the National Cybercrime Reporting Portal, which is managed by the Ministry of Home Affairs." [5]

PRIVACY RIGHTS VIS-À-VIS ONLINE AND MOBILE BANKING

[2] "Banking Regulation Act, 1949, §5"
[3] "Banking Regulation Act, 1949"
[4] "Val Srinivas and Richa Wadhwani, The value of online banking channels in a mobile-centric world, Deloitte.com (Mar. 15, 2024, 11:11 PM), https://www2.deloitte.com/content/dam/insights/us/articles/4958_Digital-banking-charticle/4958_Online-banking_Charticle.pdf."
[5] "Rimjhim Singh, Here is how much Indians lost to cyber frauds between Jan and Apr of 2024, BusinessStandard.com (Mar. 15, 2024, 11:13 PM), https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html."

In the arena of Internet and Mobile Banking, privacy is a huge concern that is rightfully raised by customers. Due to the *RBI guidelines* in place, the privacy of customers is protected to a large extent depending upon the implementation by banks in following these guidelines relating to banking in general as well as Internet banking.

Further, Online banking has opened a Pandora's box for cybercriminals to commit offences. Data breaches, data phishing, data mining as well as various types of scams affect customers and in a lot of cases, huge sums of money are deducted from their bank accounts, without them even being aware of such deductions. Breach of privacy causes irreversible damage and money loss, the cost of which is paid by either the customer or the bank, the avoidance of which is obviously desirable. Thus, statutes and legislations, along with RBI guidelines, become the necessary go-to book of solutions for all concerns relating to privacy.

Privacy Rights in India are protected under the "*Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*"[6], which were issued under the "*Information Technology Act, 2000*"[7]

- Banks are required to obtain the consent of customers before **collecting and using personal data**.

- For **data storage as well as protection**, the banks are required to have strong security practices and features in place to protect the customers' data from unauthorised access.

- Further, even in the case of **collection by third parties** of such data, the customers' consent has to be obtained specifically for such collection. The major exception to obtaining such specific consent is when it is required by law or provisions regarding banking services.

Customer awareness, however, is irreplaceable by any number of statutes as the implementation of such statutes and regulations is far from perfect. Thus, it becomes indispensable for customers to be aware of such scams that threaten their fundamental right to privacy.

[6] "The Information Technology (reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011"
[7] "Supra note 1, at 1"

RBI's GUIDELINES REGARDING SECURITY MEASURES FOR INTERNET BANKING

Online banking security is a serious concern especially prevalent in today's technologically equipped world. Protecting customers' confidential financial information while preventing access which is not authorised by customers or fraudulent activities is key to ensuring data protection and minimizing if not completely eradicating incidents of hacking.

Keeping all this in mind, all scheduled commercial banks have been issued directives as well as guidelines by the Reserve Bank of India regarding security measures to be in place for online transactions. These include:

1. **Logical Access Control Technologies:** The implementation of two-factor authentication is an important security tool that the banks are directed to implement. Methods of the aforementioned security measure include entering factors, security tokens, OTPs, and verification of biometric data. Two-factor authentication as a secure system helps enhance the security of online transactions.

2. **Encryption and secure communication:** Banks are required under these directives to incorporate the usage of encryption-based tools and technologies (e.g., HTTPS) in order to protect the data of customers during online transactions.

I. Technology and Security Standards:

1. Banks are to designate a network as well as database administrator having clearly defined roles.

2. A security policy duly approved by the Board is also to be implemented in banks while segregating the duties of Security and IT groups or divisions.

3. At the minimum, banks are required to use proxy server firewalls to facilitate high-level control. As far as sensitive systems go, a real-time security alert is also an essential.

4. Attempted or suspected security violations are to be reported by the commercial banks and follow up action is to be taken in regards to the same. Furthermore, banks are supposed to acquire such tools and technologies for monitoring systems and networks

against intrusions and attacks. These tools should be used regularly to avoid security breaches.

5. Optimization of security infrastructure and policies by banks along with educating security personnel and end users is also a direction propounded by the Reserve Bank of India.

6. Proper infrastructure is to be in place for Backing up data. Further, such data should be periodically tested by the banks to ensure its recovery without any loss of transaction.

7. Proper record keeping facilities for all bank applications is a must for legal purposes.

8. Testing and upgrading security infrastructure and systems is required by the banks keeping in mind removal of bugs, loopholes, etc to cover security as well as control in a better manner.

II. Legal Issues

1. KYC and physical verification is an obligation on the part of banks to ascertain the identity and integrity of prospective customers. Therefore, banks are to only open accounts after KYC and physical verification processes.

2. The security procedure adopted by banks for authenticating users needs to be in accordance with the Information Technology Act of 2000 (via the asymmetric crypto system and hash function) to authenticate electronic records. Other methods of authentication by banks should be recognized as a source of legal risk.

3. The banks, on account of hacking and breach of secrecy resulting in non-maintenance of privacy and confidentiality of the data of customers, should install adequate risk control measures to manage such risks.

4. Currently, in the Indian banking scenario, there is very little scope for banks to act on commands to stop payment; therefore, at the very least, the banks should at the very least clearly notify customers of the situations and time frame within which the aforementioned directions could be accepted.

5. Banks should insure themselves against the impending risks of hacking, denial of

service arising out of technological failure, etc.

III. Regulatory and Supervisory Issues:

- Only the banks that have acquired licenses and are being supervised while having a physical presence in India are permitted to deal in Internet banking services to the residents of India.

- Only the institutions who are the cheque clearing systems' members are to participate in Inter-bank payment gateways for Internet Banking.

- Further, prior approval by the RBI is required by banks to offer transactional Internet banking services. Any material changes in the products/services, every breach/failure of security systems are to be reported to the RBI.

- The products as well as services are to only be offered to account holders and not to be offered in jurisdictions other than India. The services are to only deal with local currency products.

- The only exceptions to Internet banking services being offered to residents in India are in accordance with the "FEMA (Foreign Exchange Market Act)"[8], i.e., where Indians who are residents are permitted to continue to maintain their accounts overseas.

- Indian banks' overseas branches will be permitted to offer such services subject to their satisfaction along with the satisfaction of the host and home supervisors.

- Outsourcing guidelines are to be maintained by banks to manage risks related to third-party service providers, e.g., defective or disruption in services, etc.

- The rights and liabilities of each party must be mentioned clearly in the bilateral contract between the payee and the payee's bank, participating banks, and service provider. The bilateral contract is to form the legal basis for such transactions.

- Further, through a disclosure template, the banks are supposed to make mandatory disclosures of risks, responsibilities and liabilities.

[8] "Foreign Exchange Management Act, (1999)"

NEW CHALLENGES FOR REGULATORS

Bank management, as well as regulatory along with supervisory bodies, face new difficulties as a result of this shifting financial landscape. The main causes include the rise in cross-border transactions brought about by significantly reduced transaction costs and easier banking operations, as well as the dependence on technology to give financial services the required level of security.

- **Risk related to regulations:** There is a risk that banks would attempt to evade oversight and regulation since the Internet makes it possible for services to be rendered from any location in the globe. Even banks that operate remotely via the Internet may be subject to their licensing requirements. In situations where supervision is inadequate, and collaboration between a virtual bank and the home supervisor is lacking, licensing would be especially required.

- **Legal risks:** Banks need to comply with multiple legislations in the case of e-banking and, further, are obligated by the law to be liable to customers in case of security breaches or frauds, hacking, etc., provided the customers have informed the banks well within the time limit as set by the RBI. In case of failure to compensate the customers adequately, banks may face huge losses by way of litigation or even other dispute resolution mechanisms.

- **Hacking and Frauds:** One of the many downsides of society becoming tech-savvy is how e-banking exposes and makes customers vulnerable to frauds and hacking of their bank accounts. Not a lot of customers are aware of data phishing and scams and end up revealing confidential information to avoid blackmail, extortion, or falling prey to “win the lottery” scams. Thus, making customers aware of such practices also poses a huge challenge. Thus, banking regulators and supervisors have to ensure that banks have appropriate security and prevention mechanisms in place to avoid such scams and activities.

- **Awareness limited in Rural Areas:** Although individuals and residents belonging to the middle and upper-level economies are exposed to online and mobile banking, citizens belonging to rural areas are not yet aware of these options being available for them to exercise. Further, even if there is awareness, operating such services is quite a task for these strata of society, or worse, they might fall prey to phishing activities and scams. Thus, bringing about awareness in the rural sectors of society as well is the need of the hour.

- **Reputational risk:** Security breaches and data phishing from a particular app providing online banking services or a bank's mobile banking app will indefinitely cause major reputational harm to the names associated with them. Customers might shut down their accounts because of the immense distrust that would arise in such situations and these apps may lose huge business. Even worse, customers' distrust may also translate to the name of the bank and the banking system of that bank may be seriously affected. Thus, the banks following statutory as well as RBI guidelines is a must to protect their reputation at stake in such unfortunate scenarios. Rightful compensation to the customers in case of unfortunate incidents of fraud or security breaches is also a practice that the banks should not shy away from to avoid larger ramifications.

- **Banks' Responsibilities:** Indian banks are required by law to protect the integrity, security, and confidentiality of client data and funds when conducting transactions through online banking. They must put strong safety protocols in place, protect consumer privacy, offer safe channels for transactions, and react quickly to any events or breaches of security.

- **Protections for Customers**: Customers who conduct online banking transactions are granted specific protections under Indian banking legislation. Customers' liability for unauthorised transactions is limited by the RBI's "Limited Liability for Customers in Unauthorised Electronic Banking Transactions" framework, as long as they notify the bank of the incident as promptly as possible. Depending on the type of account and the promptness of reporting, customers are usually only expected to incur the loss up to a certain sum.

- **Dispute Resolution:** Banks require a system in place to handle grievances and complaints from clients. Customers can file complaints about shortcomings in banking services, particularly those pertaining to online banking, through the Banking Ombudsman Scheme, created by the RBI.

ELECTRONIC TRANSACTIONS IN ONLINE BANKING

Electronic transactions are becoming more and more relevant and in use by the day by individuals belonging to all strata of society. Customers nowadays prefer electronic transactions to go to the banks physically because of the time that is saved and the convenience of e-banking from the comfort of their homes.

Electronic transactions in internet banking are a variety of financial activities that can be conducted online, including:

- *Fund transfers:* Transferring money between bank accounts via "electronic fund transfers (EFTs)," such as "Real Time Gross Settlement (RTGS)," or "National Electronic Funds Transfer (NEFT)."
- *Online bank transfers:* Transferring funds directly across bank accounts;
- *Digital payments:* Transferring funds between accounts using a digital device, such as a computer or smartphone;
- *Virtual payment cards:* Digital copies of actual debit/credit cards;
- *Digital wallets:* Utilising a digital wallet such as "PayPal", "Apple Pay", or "Google Pay";
- *Contactless payments:* Utilising "near field communication (NFC)" or "radio frequency identification (RFID) technology" to make payments by waving or tapping a smartphone/card that is near a terminal of payment.

Electronic transactions in India are governed by a few major laws as well as standards, rules, and guidelines. These include the following:

- **"RBI Guidelines"[9]:** In India, online banking is majorly regulated by the guidelines issued by the Reserve Bank of India. The RBI has issued various guidelines for banking in general that cover electronic banking as well. These guidelines specifically cater to customer protection, prevention, and management of frauds, risks, etc. Thus, the guidelines play a major role in governing, regulating and supervising Internet and Mobile Banking.
- **"Payment and Settlement Systems Act, 2007"[10]:** The 2007 Act provides for the supervision along with the regulation of payment systems in India. The Act also empowers the RBI in terms of regulation and establishment of online payment systems

[9] "Reserve Bank of India Guidelines, 2018"
[10] "Payment and Settlement Systems Act, 2007"

and operation standards, respectively**.** Some major examples of payment and settlement systems in India include:

- "Real-time gross settlement (RTGS)"
- "Electronic Clearing Services (ECS Credit)"
- "Credit as well as Debit cards"
- "National Electronic Fund Transfer (NEFT) system"
- "Unified Payments Interface (UPI)"

- **"Information Technology Act, 2000"[11]:** The act governs e-transactions, cybersecurity as well as e-signatures in India. It holds a significant position in legally recognising e-signatures, contracts and records, and online banking transactions, various cybercrimes such as identity and data theft. Moreover, the act also ensures that these e-records are admissible as evidence in the court. Provisions for dispute resolution of e-transactions and mechanisms for the same are also provided under the ambit of the Act making it an indispensable legislation for the purpose of Internet and Mobile banking.

- **"Payment Card Industry Data Security Standard"[12]**: The Standard is an information security standard, established by major card companies. These were first created in 2004 by 5 major credit card companies: "MasterCard", "Visa", "Discover", "American Express" and "JCB". Its primary goal is to safeguard the security of sensitive data of the cardholders such as the CVV, expiry dates as well as card numbers. Thus, these standards are instrumental in preventing as well as minimizing risks of data being breached, fraud, etc.

DIFFERENCE BETWEEN MOBILE AND INTERNET BANKING

Mobile Banking:

- Mainly, all features of mobile banking can be used only after installing the mobile

[11] "Supra note 1, at 1"
[12] "Payment Card Industry Data Security Standard, 4.0"

banking app of the customer's bank in which they hold an account.

- As compared to Internet banking, mobile banking is limited, especially when not using the mobile banking app.

- However, banks are now offering more facilities such as transfer of funds, locating an ATM, ordering a chequebook, etc.

Internet Banking:

- Internet Banking enables one to conduct online transactions through a laptop or computer with or without an Internet.

- It offers a relatively larger number of services than mobile banking, such as checking one's account statement, transferring funds from one account to another, opening a new Fixed Deposit, etc.

- Internet Banking passwords cannot be used as a substitute to bank passwords to access personal data in customers' respective banks.

"Parameters	**Mobile Banking**	**Net banking**
Device used	Smartphones, tablets	Laptop, Desktop, mobile, tablets
Services offered	Limited – lesser as compared to Netbanking	All banking services available – Most of the banking services available
How to access	Customers need to download the banking mobile application	Customers only require a User ID and password to use banking services online
Ease	Easy to use and can be used on the go	Comparatively a little difficult to perform banking services
Push notifications	Customers receive notifications regarding banking offers, exciting deals and more	Not available
Other services	Mobile banking can be access through SMS	Requires laptop, desktop and a stable internet connection" [13]

[13] "A Complete Guide About the Difference Between Net Banking and Mobile Banking, Paytm.com (Mar. 15, 2024, 11:25 PM), https://paytm.com/blog/net-banking/difference-between-net-banking-vs-mobile-banking/#h-a-comparative-difference-between-net-banking-and-mobile-banking"

LEGAL COMPLEXITIES AND CONSIDERATIONS INVOLVED IN CROSS-BORDER ONLINE BANKING

Since parties and jurisdictions outside of India are involved, cross-border online banking in India entails additional legal issues and difficulties. Among the important factors to take into account are:

- **Regulatory Compliance:** Banks that offer internet banking services across borders must abide by the laws and rules of both their home as well as their host countries. Local rules, licensing criteria, data protection legislation, and protection of consumers' standards must all be followed.

- **Issues of Jurisdiction**: Considering different nations may have distinct rules and regulations governing online banking, cross-border transactions may present jurisdictional issues. In cross-border transactions, identifying the relevant legislation, the dispute resolution jurisdiction, and the enforcement of legal remedies can be challenging.

- **Data Privacy:** Both the home and host countries' data protection as well as privacy regulations are to be taken into account when transferring customer data across international borders. In order to comply with these relevant rules and regulations, banks must make sure that client data is sufficiently protected during cross-border transfers and that adequate data transfer procedures are in place.

- **International Agreements:** In order to encourage collaboration and information sharing in financial concerns, India has signed bilateral along with multilateral agreements with a number of nations. Banks which employ cross-border online banking should think about the ramifications of these agreements and make sure that all obligations resulting from them are honoured.

LEGAL IMPLICATIONS AND REQUIREMENTS FOR ELECTRONIC TRANSACTIONS IN ONLINE BANKING

- **Electronic Signatures:** Subject to specific requirements, electronic signatures are accepted as legally valid and comparable to handwritten signatures under the

"Information Technology Act of 2000"[14]. Banks are required to make sure that their online banking systems support electronic signatures and adhere to the guidelines.

- **Legal Validity of Electronic Records:** According to the Information Technology Act, electronic records are legally recognised and can be used as evidence in court. In order to prove the legitimacy and legality of electronic records when needed, banks must keep accurate records of banking transactions that are made online.

- **Cybercrime and Fraud:** Indian banks and internet banking users should be aware of the legal ramifications of fraud and cybercrime. Financial fraud, phishing, data theft, and unauthorised access are among the offences covered by the Information Technology Act and other applicable laws. It is the duty of banks to report such instances and assist law enforcement in their investigations.

- **Consumer Protection:** Customers using internet banking are protected by Indian consumer protection laws, such as the Consumer Protection Act. Lucid information regarding terms and conditions, fees and charges, dispute resolution procedures, and channels for client complaints and remedies must be provided by banks.

- **Banks' Responsibilities:** Indian banks are required by law to protect the, security, confidentiality and integrity of client data and funds when conducting transactions through online banking. They must put strong safety protocols in place, protect consumer privacy, offer safe channels for transactions, and react quickly to any events or breaches of security.

- **Protections for Customers**: Customers who conduct online banking transactions are granted specific protections under Indian banking legislation. Customers' liability for unauthorised transactions is limited by the RBI's "Limited Liability for Customers in Unauthorised Electronic Banking Transactions" framework, as long as they notify the bank of the incident as promptly as possible. Depending on the type of account and the promptness of reporting, customers are usually only expected to incur the loss up to a certain sum.

- **Dispute Resolution:** Banks require a system in place to handle grievances and

[14] "Supra note 1, at 1"

complaints from clients. Customers can file complaints about shortcomings in banking services, particularly those pertaining to online banking, through the Banking Ombudsman Scheme, created by the RBI.

ANALYSING CUSTOMER LIABILITY IN CASE OF FRAUD EXEMPTIONS TO A GOVERNMENT COMPANY:

"Limited Customer Liability"

(a) "Zero Liability of a Customer"

When an unauthorised transaction takes place in one of the following circumstances, the customer is entitled to zero liability:

i. Contributory fraud, deficiency or negligence on the bank's side (whether or not the customer reports the transaction).

ii. Third-party breach, in which the bank is alerted by the customer within a period of three working days after receipt of the bank's notification regarding the unauthorized transaction, and further, the location of the deficiency is someplace else in the system rather than with the bank or the client.

(b) "Customer's Limited Liability"

In the following situations, a customer is responsible for any losses resulting from unauthorised transactions:

i. The customer will be responsible for the full loss until he notifies the bank of the unauthorised transaction if the loss results from his negligence, such as when he revealed the payment credentials. It will be the responsibility of the bank for any such losses that arise after the unauthorised transaction has been reported.

ii. If the bank is notified of the unauthorised e-transaction, the customer within 4-7 (working) days after the receipt of notification of the transaction, and neither the customer nor the bank is to blame for the transaction, the customer's liability for each transaction is limited to the amount of the value of the transaction or the figure listed in "Table 1", out of these, which is lower.

Additionally, the liability of the customer will be assessed in accordance with the approved policy of the Bank's Boad if the reporting delay exceeds seven working days. At the time of account opening, banks must disclose the specifics of their liability policy, which is developed in consonance with the guidelines of the RBI. For broader circulation, the banks must also post their authorized policy in the public domain. Additionally, each current customer needs to be personally notified of the bank's policy.

"Table 1" **Maximum Liability of a Customer under paragraph 7 (ii)**	
Type of Account	**Maximum liability (₹)**
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/Cash Credit/Overdraft Accounts of MSMEs • Current Accounts/Cash Credit/Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs. 5 lakh	10,000
• All other Current/Cash Credit/Overdraft Accounts	25,000" [15]

Table 2 summarises the client's overall obligation for third-party breaches, provided the defect is not with either the customer or the bank but rather in the system somewhere. The number of working days listed in Table 2 will be determined by the customer's home branch's business schedule, omitting the day the message was received:

[15] "DCBR.BPD. (PCB/RCB). Cir.No.06/12.05.001/2017-18"

"Table 2" **Summary of Customer's Liability**	
Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (₹)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in **Table 1**, whichever is lower
Beyond 7 working days	As per bank's board approved policy,"[16]

REVERSAL TIMELINE FOR CUSTOMER ZERO LIABILITY/LIMITED LIABILITY

Within ten days (which are working) of the notification of the customer (shadow reversal), the amount that was involved in the electronic transaction, which was unauthorized, will be credited by the bank to the customer's account (without waiting for the settlement of any insurance claims). Value-dating the credit to the date of the unlawful transaction is required. Even in circumstances of the customer's fault, banks have the authority to choose to waive any duty owed by customers in the event of unauthorized electronic banking activities.

In addition, banks must make sure that:

i. a complaint is settled, the customer's liability is determined. Further, the customer shall be compensated within a time frame that may be stated in the bank's Board-approved policy, but no later than 90 days from the date of complaining;

ii. if the bank has failed to rectify the complaint or determine the customer's liability within that time frame, the customer receives the compensation at once; and

iii. The interest is not lost by the customer in the situation of a debit card or bank account, and does not incur any additional interest burdens in the instance of a credit card.

[16] "DCBR.BPD. (PCB/RCB). Cir.No.06/12.05.001/2017-18"

Lastly and importantly, the burden of proof with respect to the liability of the customer in circumstances which involve unauthorised e-banking transactions lies with the bank.

RELEVANT JUDGMENTS

1. "**Hemant Kanoria v. Bank of India:**

   The Calcutta High Court notably held that the purpose of the Master Directions, framed under Section 35A of the Banking Regulation Act, 1949, enumerated in the Master Directions, is to provide a framework to Banks enabling them to detect and report frauds early and taking timely consequent actions like reporting to the investigative agencies so that fraudsters are brought to book early, examining staff accountability and do effective fraud risk management.

   The Court further held that the Directions aim to enable faster dissemination of information by the RBI to Banks on the details of frauds, unscrupulous borrowers and related parties based on Banks' reporting so that necessary safeguards/preventive measures by way of appropriate procedures and internal checks may be introduced and caution exercised while dealing with such parties by Banks"[17]

2. **"Central Bureau of Investigation, Bank Securities and Fraud Cell v. Mulangi Krishnaswamy Ashok Kumar:**

   The Bombay High Court while observing the "phenomenal rise in magnitude of white-collar crimes" especially scams and the "outdated legal provisions that treat a Rs. 500 defrauding by a Government servant in grade III and those looting and plundering Rs. 500 crores as being on the same footing" observed that it had shocked the conscience of the people and there are growing feelings amongst them that regulatory watchdog agencies are incapable to prevent and check such evils or deliberate corroborators to the same.

   The Court emphasized the necessity of white-collar crimes involving high stakes, which are committed with cool calculations and deliberate design, with an eye on personal profit, regardless of the consequences to the community being dealt with an iron hand."[18]

[17] "Hemant Kanoria v. Bank of India, 2024 SCC OnLine Cal 1012"
[18] "CBI Bank Securities and Fraud Cell v. Mulangi Krishnaswamy Ashok Kumar, 1999 SCC OnLine Bom 179"

3. "***Justice KS Puttaswamy v. Union of India:***

The Supreme Court, in this landmark judgment, led by a 9-judge bench, held that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. Further, it held that informational privacy is included as a facet of the right to privacy. It also observed that the dangers to privacy in an age of information can originate from the state and non-state actors.

The Hon'ble Apex Court also recommended to the Union Government the need to examine and put into place a robust regime for data protection. Emphasis was placed on such a regime requiring a careful and sensitive balance between individual interests and legitimate concerns of the state like protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits.

The Hon'ble Court also notably observed and held that in an era where there are wide, varied, social and cultural norms and more so in a country like ours which prides itself on its diversity, privacy is one of the most important rights to be protected both against State and non-State actors and be recognized as a fundamental right"[19]

CONCLUSION AND SUGGESTIONS

Although Online and Mobile Banking have come a long way in the 21st century, secure e-banking still has a long way to go. The number and quality of statutes can only help secure digital banking to an extent. We require the aid of policymakers, Governments, Banks and experts to help promote safe and secure online and mobile banking. Further, such safe and secure e-banking must reach each nook and corner of society via awareness and government schemes.

1. Conduction of surveys of the customers as well as cyber-criminals in each state for aiding in the formulation of policy for raising customer awareness and reducing the cyber-crime rate.

[19] "Justice KS Puttaswamy v. Union of India, 2017 SCC OnLine SC 996"

2. Specific policies and schemes should be designed by the Central as well as State Governments and experts in the field of banking, law, IT, and cyber-crime with respect to raising customer awareness, keeping in mind the cyber-crime rate for each state and on the basis of surveys conducted as aforementioned, as well as increasing the number of online and mobile banking users through such schemes.

3. Designate supervisory authorities to conduct regular surprise visits to check the security mechanisms in place as well as the guidelines and statutory requirements being followed to a tee, by banks in online and mobile banking. Further, submission of a biannual report by such supervisory authorities shall also be made mandatory and available to the public.

4. Conduct awareness programmes state and district-wise, especially in rural areas, to help each stratum of society get uplifted and learn how to use online and mobile banking while also being aware of the precautions and preventions they should take to help mitigate the risks of cybercrime.

5. Banks to mandatorily educate their customers of the bank's policies and timeline, during which customers are supposed to report frauds and other practices relating to breaches of privacy and security. Furthermore, banks should also educate customers regarding the liability of customers with respect to the time taken to notify the bank in case of frauds being committed against their customers.

REFERENCES

- "Monisha, Kanika Bhudhiraja, Jatinder Kaur, 2017, Electronic Banking in India: Innovations, Challenges and Opportunities, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCIETM – 2017 (Volume 5 – Issue 11)
- Michelle Julka, *Legal Challenges in Regulating Online and Mobile Banking Security: Cybersecurity and Customer Trust* (2025)
- BankofBaroda.com
- RBI Guidelines (2017-18)
- Business Standard
- Paytm.com
- Deloitte.com
- Business Standard.com
- International Monetary Fund (IMF.org)
- idfcfirstbank.com