DRAFT

Finance and Privacy

Contents

DRAFT
Introduction

Financial privacy involves the protection of consumers from unlawful access to financial accounts by private and public bodies, and the unlawful disclosure, sharing, or commercial use of financial information. Types of financial institutions which can collect/access financial information include: banks, tax collectors, mortgage lenders, investment advisers, insurance companies, and real estate brokers. Typical types of financial transactions that consumers can engage in include: paying taxes, buying property, opening bank accounts, and investing in markets. In India this list expands to include micro-credit transactions, rural banking, transactions with banking intermediaries, transactions with money lenders & indigenous bankers, Chit funds, Nidhis, and mutual benefit funds. Violations of privacy in the financial sector have the potential to cause serious damage due to the highly sensitive information that is recorded, exchanged, and retained. Individuals must trust financial institutions with a range of personal identifying information like their financial records, access to information held in their accounts, and their credit history — each of which can be used either directly by banks and their employees, or indirectly by individuals — for wrongful gain. Furthermore, government agencies such as the Income Tax department collect large amounts of personal information, and records accumulated in the course of these proceedings could violate an individual's privacy.

In addition to the above, the fact that Indian companies now offer outsourced financial services to financial institutions abroad vastly expands and globalizes the number of people who could be affected by violations of privacy in the Indian financial sector. For countries that have enacted financial privacy legislation, the laws often work to place the control of financial information into the hands of consumers. Institutionally these are done through authorized consents, privacy policies, and opt in/opt out notices. In India, the practice of financial privacy is still taking hold. A 2010 DSCI survey on financial privacy in India found that the percentage of Indian banks publishing privacy policies is still very low, and that the lack of consumer awareness and education also serve as obstacles to strong financial privacy practices in India.[1] Finally, the introduction of e-finance and e-governance schemes come with the promise of universalizing financial services, but could also turn, if the privacy implications are not carefully weighed, into a concentrated source of financial information for control and misuse. In this context, and in light of the rapid digitization that the financial sector in India is undergoing, this chapter will discuss the ways — old and new— in which financial privacy can be compromised, review what legal safeguards for privacy exist in India, and make recommendations for additional safeguards at both the level of each legislation, and broadly for the financial sector in India.

1. DSCI - KPMG Banking Survey Report – Final.pdf http://www.dsci.in/sites/default/files/DSCI%20-%20KPMG%20Banking%20Survey%20Report%20-%20Final.pdf

Legislation

In India the privacy of financial information is protected through legislation, through banking customs, guidelines and norms, and through relevant policies. Applicable Indian legislation that provides privacy protection over financial information includes the following.

The Negotiable Instruments Act, 1881[2]

This Act regulates commercial transactions (between banks and individuals as well as between individuals only) completed through 'negotiable instruments'. Prior to the Act's passage, transactions made by "negotiable instruments" were regulated under the Indian Contract Act, 1872 and customary trade law. A “negotiable instrument” means a promissory note, bill of exchange, or cheque payable either to order or to the bearer. Negotiable instruments, therefore, are money/cash equivalents. The Act extends to the whole of India except for the State of Jammu and Kashmir. The provisions being discussed here are intended to determine who should be held liable when payment is made using a fraudulent cheque and establish the duties of banks for verification. Thus, the provisions pertain to privacy to the extent that they work to protect against fraud. Because the Act speaks only to liability, the principles of choice and consent, collection limitation, purposes limitation, access and correction, openness, security, oversight, notice and disclosure of information may not be applicable. The privacy principles are applicable in the following ways:

Penalty/Offense/Liability/Redress

- *Liability:* A banker acting in good faith and without negligence will not be held liable for receiving a fraudulent cheque.[3] Similarly, banks are not liable to fulfill payment of a fraudulent cheque.[4]

Quality and Verification

- *Verification*: It is the duty of the Bank to verify the genuineness of the (electronic image) of the cheque and to detect any fraud, forgery, or tampering. [5]

Missing Principles

- Accountability

The Prevention of Money Laundering Act, 2002[6]

Money laundering is the process of disguising illegal sources of money in order to make it appear that the money originates from legitimate sources. Preventive measures against

---

[2] The Negotiable Instruments Act, 1881. Available at: http://chddistrictcourts.gov.in/THE%20NEGOTIABLE%20INSTRUMENTS%20ACT.pdf

3. Negotiable Instruments Act, 1881 Section 131

4. *Id.*, Section 85 (1)

5. *Id.*, Section 58

5. Id. section. 131 – inserted by Act 55 of 2002 s. 6.

[6] Prevention of Money Laundering Act 2002. Available at : http://fiuindia.gov.in/pmla2002.htm

money laundering taken by governments include the monitoring of banking customers and their business relations/financial transactions, verification of new customers, and automatic tracking of suspicious transactions. Thus, the individual's interests in financial privacy compete with the interests of the government and investigative agencies in requiring the disclosure and monitoring of financial information.

The Prevention of Money Laundering Act, 2002 was passed in an attempt to curb money laundering. The Act establishes and delegates investigative powers to various separate authorities viz. Director; Deputy Director and Assistant Director (all appointed under Section 49(1) of the Act); officers of the Customs and Central Excise Departments; officers appointed under sub-section (1) of section 5 of the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985); income-tax authorities under sub-section (1) of section 117 of the Income-tax Act, 1961 (43 of 1961); officers of the stock exchange recognized under section 4 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);officers of the Reserve Bank of India constituted under sub-section (1) of section 3 of the Reserve Bank of India Act, 1934 (2 of 1934);officers of Police; officers of enforcement appointed under sub-section (1) of section 36 of the Foreign Exchange Management Act, 1973 (40 of 1999); officers of the Securities and Exchange Board of India established under section 3 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); officers of any other body corporate constituted or established under a Central Act or a State Act; (j), such other officers of the Central Government, State Government, local authorities or banking companies as the Central Government may, by notification, specify, in this behalf.

Additionally, the Act puts in place an appellate tribunal meant to receive complaints of aggrieved persons. Individuals who commit offenses under the Act are held criminally liable. The provisions of the Act are intended to have effect not withstanding anything inconsistent that is in any other law in force at the time.[7] Given that this Act establishes powers of investigation for crimes of money laundering, the principles of choice and consent will not apply. The privacy principles are applicable in the following ways:

Oversight

- *Director, Deputy Director, and Assistant Director:* Has the power to carry out investigations with authorization by the Central Government. Directors can only undertake investigation if they have reasons recorded in writing and believe that an individual possesses money or goods achieved through the commission of a crime ("proceeds of crime") or that an individual has been charged with committing certain offences specified in the schedule to the Act. If these conditions are met, Directors have the power to provisionally attach property for a period of 150 days,[8] has the power to call for records, and impose fines.[9] For the purpose of levying a fine, the Director has the same powers as are vested in a civil court in respect of certain matters.[10]
    - *Power to make inquiries:* The Director, on his own motion or on an application by any authority, officer or person, call for records which are

[7] Id Section 71
[8] Id. Section 5
[9] Id. Section 13
[10] Id. Section 50

required to be maintained under the Act, and make inquiries as he sees fit.[11]

- *Search & Seizure:* The Director (or any other person authorized by him, not below the rank of a Deputy Director)[12] is given the power of search and seizure, allowing him/her to:
    - 1. enter and search any building, place, vessel, vehicle, or aircraft
    - 2. Break open the lock of any door, box, locker, safe etc
    - 3. Seize any record or property
    - 4. Examine on oath any person who is found to be in possession or control of any record relevant for the purposes of investigation under this Act.[13]

  Safeguards to this power include the requirement that a report must be forwarded to a magistrate under section 157 of the Cr.P.C.,[14] the authority must forward a copy of the reasons recorded along with the material in his possession to the Adjudicating Authority.[15] Furthermore, any authority authorized by the Central Government by a general or special order may search an individual and seize records or property which may be useful or relevant under the Act.[16] Safeguards to this power include the requirement that a report must be forwarded to a magistrate under section 157 of the Cr.P.C.[17],the Authority will conduct the search in front of at least two witnesses,[18] prepare a list of record or property seized and obtain signatures from witnesses.[19]
- *Search and Seizure without warrant:* The Director, if satisfied based on information discovered on the completion of a survey, that any evidence will or is likely to be concealed or tampered with, may enter the building or place and seize the evidence. This search does not require prior authorization, but the authority must record his reasons in writing.[20]

- *Adjudicating Authority*: Has the same powers as a civil court in respect of certain matters[21]. Every proceeding carried out by the adjudicating authority is considered a judicial proceeding under section 193 and 228 of the Indian Penal Code.[22]
- *Appellate Tribunal and Bench*: Established to hear appeals against orders made by the Adjudicating Authority,[23] and has the same powers as a civil court in respect of certain

---

[11] Id. Section 13(1)

12. *Id section* 48 'The Act has three classes of authorities 1. Director or Additional Director or Joint Director 2. Deputy Director, 3. Assistant Director 4. other such officers that maybe appointed under this Act. Section 50 'The Director shall have the same powers as are vested in a civil court. The additional director shall have the power to summon any person whose attendance he considers necessary to produce documents . The Assistant Director shall not (a) impound any record without recording his reasons for doing so (b) retain any record without prior permission from the Director.

13. *Prevention of Money Laundering Act, 2002, s.* 17 (1).

14. Id. section 17 (1), *Proviso*.

[15] Id. Section 17(2)

[16] Id. Section 18(1)

[17] Id. Section 18(1), *Proviso.*

[18] Id. Section 18(6)

[19] Id Section 18(7)

20. Id. Section 17(3).

[21] Id. Section 11

[22] Id. Section 11(3)

[23] Id. Section 25

matters.[24] Any individual aggrieved by the decision of the Appellate Tribunal may file an appeal with the High Court within sixty days of the communication of the decision.[25]

- *Power of Survey:* Any 'Authority' authorized under the Act has the power of survey to enter into any place where it believes any offence of money laundering has been committed[26] and inspect records[27], place marks of identification on the records inspected by him, make copies of the records inspected by him, record the statement of any person present, and ask for the furnishing of information.[28] The 'Authority' can only enter into a place on the basis of material in his possession, and for reasons recorded in writing. His/her search must also be limited to the area and for the purpose assigned.[29] Furthermore, the 'Authority' must forward a copy of the reasons that were recorded along with material collected in his possession to the Adjudicating Authority in a sealed envelope and by means which are prescribed by the Adjudicating Authority.[30]

Disclosure

- *Pro-active Disclosure*: Banking companies, financial institutions, and intermediaries must furnish retained information to the 'Director'. How and by what procedure this information should be furnished and maintained is to be determined by the Central Government in consultation with the Reserve Bank.[31] As per the RBI Master Circular regarding reporting of such transactions (discussed later in this chapter), the 'Director' means the Director, Financial Intelligence Unit-India (FIU-IND).
- *Disclosure in the public interest*: Any information received or obtained by a Director or any other authority may be disclosed to any authority, officer or body performing any functions under law, if it is determined to be in the public interest.[32]
- *Disclosure to foreign powers*: The Central Government may enter into an agreement with another Government for the exchange of information for the prevention of an offence.[33]

Access and Correction

- *Copies of retained records:* The person from whom records were seized under the Act has the right to obtain copies of the records.[34]

Collection Limitation

- *Retention of Evidence***:** Records[35] obtained through a Survey or through Search and

---

[24] Id. Section 35
[25] Id. Section 42
26. Id. Section 16 (1).
27. Id. Section 16(1)(i).
28. *Id. Section* (16)(3)(i) to (iii).
29. Id. Section 16(1)(i) and (ii).
[30] Section 16(2).
31. *Id. Section* 15. The details of the transactions which need to be disclosed are discussed later under the Disclosure section of the Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002
32. Id. Section. 66.
[33] Id. Section 56(b)
[34] Id. Section 21(2)
[35] Records: Include the records maintained in the form of books or stored in a computer or such other form as may be prescribed (Section 2(w)).

Seizure may be retained by authorities only for three months.[36]

- *Procedure for Retention:* After a period not exceeding three months, the records must be returned to the individual unless the Adjudicating Authority permits it to be stored longer,[37] or the Director appeals the decision to return the retained records[38], the Adjudicating Authority, before directing retention, must ensure that the records are required to be retained.[39]
- *Retention of Transaction Records*: Banking companies, financial institutions, and intermediaries must maintain records of their client's transaction details including location and sum of money and the identity of the relevant client.[40] The records relating to the identity of the client are to be retained for a period of ten years after the client has completed its last transaction with the banking company and records relating to transactions are to be kept for a period of ten years from the date of the transaction.[41]

Security:

- *Maintenance of Records*: The manner and procedure of maintaining and furnishing information will be determined by the Central Government, in consultation with the Reserve Bank of India.[42]

Penalties/Offenses/Redress

Offenses	***Fines***	***Imprisonment***
Any officer or authority which conducts a vexatious search without reasons recorded in writing	*Extend to fifty thousand rupees*[43]	*Two years*
Any person who furnishes false information or fails to provide information	*Extend to fifty thousand rupees*[44]	*Two years*

- *Redress:* Only banks, financial companies, and intermediaries hurt or damaged by any order made by the Director may appeal and seek redress to the Appellate Tribunal. By not extending the ability to seek redress under the Act to individuals, the Act does not sufficiently protect the privacy of the individual[45.]
- *Presumption of ownership and acceptance as evidence:* The Act assumes that where records are found in the possession or control of an individual, those records shall be presumed to belong to the person, the records are true, and will accept the record as

---

36. Section 21(1).
37. Id. Section 21(3)
38. Id. Section 21(6)
39. Id. Section 21(4)
40. *Id. section* 12 (1).
41. *Id. section* 12(2).
42. Id. Section 15
43. Id. Section 62
44. Id. Section 63
45. Id. Section 26.

evidence.[46] Further, it will be the responsibility of the accused to prove innocence.[47]

Missing Principles

- Accountability
- Openness
- Purpose Limitation
- Choice and Consent
- Notice
- Quality/Verification

The Bankers' Books Evidence Act, 1891[48]

The Bankers' Books Evidence Act, 1891 was passed to give a higher evidentiary value (*prima facie evidence*) with respect to records, documents, and books kept by banks -referred to as 'Bankers Books' in the legislation. The Act lays out broad safeguards and protections establishing how Bankers Books should be secured and how Bankers Books can be used. As this Act speaks to the maintenance and security of banker's books the principles of consent and choice, access and correction, purpose limitation, collection limitation, penalty/offences and liability, accountability and notice will not apply. The principles of privacy are applicable in the following ways:

Quality/Verification

- *Authenticity of Data:* Any printout of an entry in a Bankers Book must be accompanied with a certificate from the principal accountant or branch manager noting that the printout is indeed a printout of the relevant entry.[49]
- *Accuracy of Data:* Any printout of an entry in a Bankers Book must be accompanied with a certificate from the person in charge of the computer system vouching that to the best of his knowledge he was provided with all the relevant data and that it is reflected accurately on the print out.[50]

Security

- *Security of Data*: A certificate must also be made by the person in charge of the computer system containing a description of the safeguards put in place to: ensure that data is entered only by authorized individuals, prevent and detect unauthorized changes in data, retrieve data that is lost due to system failure or for other reasons, the manner in which data is transferred from the system to various forms of removable media, the mode of verification in order to ensure that data has been accurately transferred to such removable media, the mode of identification of such data storage devices, the arrangements for the storage and custody of such storage devices, the safeguards to prevent and detect any tampering with the system, and any other factor which will vouch

[46] Id. Section 22.
[47] Id. Section 24
[48] Bankers Book Evidence Act, 1891. Available at: http://www.vakilno1.com/bareacts/Laws/The-Bankers-Book-Evidence-Act-1891.htm
49. Id. section 2A(a).
50. Id. section. 2A(c).

for the integrity and accuracy of the system.[51]

Disclosure

- *Disclosure of information*: Banks are not compelled to proactively or reactively produce a Bankers Book in a case to which the bank is not a party to prove the transactions and contents found in a Bankers Book – unless ordered to do so by a court or judge.[52] When a court or judge[53] does allow for a Banker's Book to be inspected, the bank must certify that it is making available all related entries.

Missing Principles:

- Oversight
- Openness

The Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002[54]

This Act was enacted to enable banks and financial institutions to recover debts secured by moveable and immovable property without recourse to the Courts or any Tribunals. Under this Act, a "secured creditor" whose debt is unpaid is entitled to take possession of the assets which have been mortgaged to secure to the loan or take over the management of the business of the borrower.[55] Since the Act mostly governs enforcement of security interests, the principles of collection limitation, choice and consent

Oversight

- *Power to call for information*: The Reserve Bank may call for information relating to the securitization or reconstruction company's business or affairs at anytime from a securitization or reconstruction company.[56]

Disclosure

- *Creation of Register*: A Central Register is to be created by the Central Government for maintaining the details of transactions related to: securitization of financial assets, reconstruction of financial assets, and creation of security interests. The details maintained in the Register must be filed within thirty days of a transaction.[57] Whenever the terms or conditions or the extent or operation of any security interest registered under the Act, is modified, it must be updated in the Register.[58]
- *Public Access*: The information stored in the Central Register will be open to any person on payment of a fee in either hardcopy or electronic form.[59]

---

51. Id. Section 2A(b).
52. *Id.*, Section 5' Case in which officer of bank cannot be compelled to produce books.
53. *Id.*, Section 6, Inspection of Books by Order of Court or Judge.

[54] The Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002. http://www.drat.tn.nic.in/Docu/Securitisation-Act.pdf

[55] Section 13.

[56] Section 12A

[57] Section 23

[58] Section 24

[59] Section 26

Security

- *Records in the Central Register*: The records in the central register can be stored fully or partially on computers, floppies, diskettes, or in any other electronic form subject to such safeguards as prescribed.[60]

Notice

- *Notice to discharge debt*: The secured creditors are required to give the borrowers a notice of 60 days to pay their debt before the secured creditor can enforce any of its rights under this Act.

Penalty/Liability/Redress

- *Right to appeal*: Any aggrieved individual can submit a complaint against any action taken by a secured creditor under section 13(4), to the Debts Recovery Tribunal along with a fee. [61] If the individual is not satisfied with the order made by the Debts Recovery Tribunal, they may appeal the order to the Appellate Tribunal.[62]
- *Right to receive compensation*: If ordered and as determined by the Debts Recovery Tribunal, the Court of a District Judge, or the Appellate Tribunal, or the High Court, a borrower is entitled to compensation if possession of its secured assets was taken wrongfully.[63]

Missing Principles

- Openness
- Verification and Quality
- Purpose Limitation

Case Laws

K.J. Doraisamy v. *Asst. General Manager*,[64] (2006)

The right of a Bank to adopt any lawful method for the recovery of its dues, can sometimes come directly into conflict with the right to privacy and dignity of the borrower, which has now come to be recognised, to some extent, as part of the right to life guaranteed under Article 21 of the Constitution. In the case of *K.J. Doraisamy* v. *Asst. General Manager*,[65] the bank wanted to recover its loan by bringing the security given for the loan for sale by publishing its details including the photograph of the defaulter in news papers. This action of the Bank which was threatened under Section 13 of the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act was challenged by the borrower as being an infringement of the right to privacy of the borrower. Deciding the above issue in favour of the bank the High Court of Madras held as follows:

[60] Section 22
[61] Section 17
[62] Section 18
[63] Section 19
[64] http://judis.nic.in/judis_chennai/qrydisp.aspx?filename=8673
[65] http://judis.nic.in/judis_chennai/qrydisp.aspx?filename=8673

"29. The above discussion makes it clear that from the point of view of the individual, his right to privacy is not absolute and from the point of view of the Bank, the duty to maintain secrecy is superceded by a larger public interest as well as by the Bank's own interest under certain circumstances.

……..

32. If borrowers could find newer and newer methods to avoid repayment of the loans, the Banks are also entitled to invent novel methods to recover their dues. Moreover, the petitioner is not entitled to seek the relief of a writ of mandamus for the following reasons also:- (a) It is a fundamental principle of the Law of Writs that a Writ of Mandamus can be issued only to compel the performance of a statutory or public duty. But the prayer made in the present writ petition is to prevent the Bank from the performance of its public duty. (b) What is challenged in the present writ petition, is a notice under section 13 of the SARFAESI Act. The petitioner has a statutory remedy of appeal under section 17 of the Act, without exhausting which, he is not entitled to invoke the writ jurisdiction of this court. Hence I find no violation of any right or legal provision in the threat held out by the respondent Bank to publish the photographs of the borrower and the surety for the non repayment of the loan. Consequently the writ petition fails and is dismissed."

The Court in this case also quoted the Judgment in *Francis Coralie Mullin v. The Administrator, Union Territory of Delhi*,[66] to link the extent of the right to life with that of the economic development of the country in the following words:
"We think that the right to life includes the right to live with human dignity and all that goes along with it, namely, the bare necessities of life such as adequate nutrition, clothing and shelter over the head and facilities for reading, writing and expressing oneself in diverse forms, freely moving about and mixing and commingling with fellow human beings. ***Of course, the magnitude and content of the components of this right would depend upon the extent of the economic development of the country,*** but it must, in any view of the matter, include the right to the basic necessities of life and also the right to carry on such functions and activities as constitute the bare minimum expression of the human-self."

It is also significant to note that this case relies upon English law and precedent to come to a conclusion that the duty of the Bank to maintain secrecy can be superseded by the Bank's own interest, however the Court has not defined exactly what it means by Bank's interest, although it seems that the Court is trying to link the bank's interest with the state of the economy and therefore perhaps trying to say that serving the interest of the bank would mean serving the interest of the public in general.

Case Highlights

- ***The Court seems to indicate that the 'banks' interest' would serve the interest of the economy in general and hence might serve the "public interest" as well***
- ***The Court seems to have discussed both the right to privacy as well as the bank's duty of confidentiality and secrecy and while it has only said that the***

[66] http://www.indiankanoon.org/doc/78536/

right to privacy is not absolute, it has laid down 'larger public interest' and 'banks own interest under certain circumstances' as the exceptions to the confidentiality/secrecy.

- ***The bank can publish the photographs of borrowers who have not paid loans***
- ***Does not mention proportionality except when quoting an English precedent***

Venu P.R. v. *Assistant General Manager, SBI and another*,[67] (2013)

However subsequently a Single Judge Bench of the Hon'ble Kerala High Court in *Venu P.R.* v. *Assistant General Manager, SBI and another*,[68] acknowledged the position adopted by the Madras High Court in *K.J. Doraiswamy* but disagreed with it on the ground that there is no provision in law which allows the bank to publish the photographs of defaulters in newspapers. Although this decision was given in the context of a public sector bank (substantially owned by the government) the Court did say that the situation might be different if it involved private financiers:

> "A public authority like the bank has the power to realise the dues only in a manner authorised by law quite unlike a private financier who can resort to any step unless forbidden by law. Situation may be different where the loanees are proclaimed offenders and are absconders fleeing away from the clutches of law in which case the publishing of their photographs might be justified. Otherwise the threat held out by the banks to publish the photographs of loanees in leading newspapers on their failure to repay the debt within a specified date lacks legislative sanction and is wholly illegal and arbitrary."

Saying that such an action might infringe the right to privacy of the defaulters the Court held that:

> "There is nothing immoral in being unable to repay the loans availed of owing to the floundering of business or due to some other unavoidable reason which can enable the bank to infringe the right to privacy of loanees. There is no compelling public interest warranting the publishing of the photographs of the loanees in newspapers in which case only the right to privacy has perhaps to give way. Some of the loanees may even be driven to commit suicide for fear of ignominy on publishing their photographs in newspapers at the instance of the bank and it will remain a permanent taboo for their family. The publishing of the photographs in newspapers for the inability to clear the loan arrears to the bank in time is clearly an affront to the right to live with dignity and honour as well as the right to privacy of the loanees. I have no hesitation to hold that publishing the photographs by the bank under such circumstances is violative of the rights guaranteed to the loanees under Article 21 of the Constitution of India."

When the Court says that "There is nothing immoral in being unable to repay the loans availed of owing to the floundering of business or due to some other unavoidable reason

[67] 2013 (132) AIC 612 (Ker.H.C.)
[68] 2013 (132) AIC 612 (Ker.H.C.)

which can enable the bank to infringe the right to privacy of loanees", it seems that the Court in this case is trying to bring in morality as a test or a circumstance to determine whether the privacy of the individual can be infringed. Further the Court says that " Situation may be different where the loanees are proclaimed offenders and are absconders fleeing away from the clutches of law in which case the publishing of their photographs might be justified." Does this mean that if a person has committed immoral acts or is a proclaimed offender then he loses his right to privacy or that immoral people have lower privacy rights than moral individuals.

Case Highlights

- ***A public sector bank does not have the right to publish pictures of defaulting borrowers in the newspapers;***

- ***There is nothing immoral in being unable to repay the loans due to some unavoidable reason which can enable the bank to infringe the right to privacy of loanees.***

- ***There is no compelling public interest warranting the publishing of the photographs of the loanees in newspapers.***

- ***A public authority like the bank has the power to realise the dues only in a manner authorised by law quite unlike a private financier who can resort to any step unless forbidden by law.***

- ***This case does not mention the Bank's duty of secrecy or confidentiality or the doctrine of proportionality.***

Foreign Contribution Regulation Act, 2010

The Foreign Contribution Regulation Act of 2010[69] aims to regulate the acceptance and utilisation of foreign contribution or foreign hospitality by certain persons by empowering the government to prohibit contributions towards any activities detrimental to the national interest and for matters connected therewith or incidental thereto.[70] In the context of the Act, 'foreign contribution' refers to donations and transfers of any article, currency or security made by foreign sources while foreign hospitality refers to the offering of providing a person with the costs of travel to a particular county with free boarding, medical treatment, etc. Taking into account the purpose and scope of the Act, the principles of choice and consent, notice, openness,

Collection Limitation

- *Power call for Records*: Under the Act, the government is conferred with the power to call for otherwise confidential financial information relating to foreign contributions of

[69] Research completed by Tarun Krishnakumar

70. Preamble to the Foreign Contribution Regulation Act, 2010.

individuals and companies if satisfied that acceptance of such contribution or hospitality would prejudicially affect:

- The sovereignty and integrity of India; or
- Public interest; or
- Freedom or fairness of election to any Legislature; or
- Friendly relations with any foreign State; or
- Harmony between religious, racial, social, linguistic or regional groups, castes or communities.[71]

- *Proactive Disclosure*: Entities registered under the Act are required to report to the Central government and any authority as may be specified, the amount of foreign remittance, the source and manner of receipt of the funds and other particulars in such form as may be prescribed.[72] Any candidate for an election who has received any foreign contribution during the 180 days immediately preceding his nomination is required to report to the Central government or a prescribed authority or both, the amount of foreign remittance, the source and manner of receipt of the funds and other particulars in such form as may be prescribed.[73]
- *Power to Audit*: The Central Government has the power to authorize any officer holding a Group A post, to audit the accounts of any entity registered under the Act and such officer has the power to enter any premises after sunrise and before sunset for the said purpose.[74]

Oversight

- *Proactive Disclosure*: Banks are required to report to the authority as may be specified, the amount of foreign remittance, the source and manner of receipt of the funds and other particulars in such form as may be prescribed.[75]
- Foreign Contribution: No member of a Legislature, office bearer of a political party, judge, government servant can accept any foreign hospitality without the prior permission of the Central Government.[76]

Offenses	***Fines***	***Imprisonment***
Giving false information in its intimation or in its registration application[77]	*Yes*	*Six months*
Any person who furnishes contravenes or assists in contravening the provisions of the Act in relation to an article, currency or security	*Rupees One thousand or five times value of the article, security or currency*[78]	*Two years*
Any person who furnishes	*Yes*[79]	*One year*

71. Proviso to Section 9 of the Foreign Contribution Regulation Act, 2010.
72 *Id.* Section 17(2).
73 *Id.* Section 21.
74 *Id.* Section 20.
75 *Id.* Section 17(2).
76 *Id.* Section 6.
77 *Id.* section 33.
78 Id. Section 34
79 Id. Section 34

contravenes or assists in contravening the provisions of the Act		

Missing Principles

- Disclosure
- Security
- Openness
- Verification and Quality
- Purpose Limitation
- Choice and Consent
- Notice
- Oversight
- Notice
- Penalty/Liability/Redress

Credit Information Companies (Regulation) Act, 2005[80]

Violations of privacy with respect to credit information arise when credit agencies share and exchange reports with insurers and employers. Based on this information entities can use the information to deny services and opportunities to individuals. The Credit Information Companies (Regulation) Act establishes the credit information companies to govern and regulate the use of individuals' credit information. Credit information under the Act includes the amounts and nature of loans, the nature of securities taken, the guarantee furnished or any other non-funding based facility granted by a credit institution to establish the creditworthiness of any borrower.[81]

Within the Act there are four bodies that handle and process credit information: the credit information company[82], the credit institutions, State Bank of India, national banks etc.[83], the specified user[84], and the individual provider of information. The Credit Information Company (which is registered with the Reserve Bank of India) collects and processes information on the trade, commercial and financial standing of borrowers of credit institutions and then provides the same to specified users (which include credit information companies and credit institutions) and credit institutions as well as the person whose information is being collected and processed.

Broadly the Act requires privacy principles to be adhered to by every credit institution, credit information company, or specified user must set in place a system to regulate the collection,

[80] Credit Information Companies (Regulation) Act 2005. Available at: http://www.lawzonline.com/bareacts/credit-information-companies-regulation-act/credit-information-companies-regulation-act.html

81. Id. section 2 (d)
82.Id. Section 2 (e).
83. Id Section 2 (f).
84. Id. Section 2(l).

processing, collating, recording, preservation, secrecy[85], sharing, and usage of credit information.[86] Specifically:

Verification, Security and Disclosure

- the requirement to ensure that credit information is accurate, complete, and protected against loss, use, or unauthorised disclosure;[87]

Verification

- the extent of the obligation to check the accuracy of credit information before disclosing it to credit information companies, credit institutions, or specified users;[88]

Retention

- how credit information should be maintained, including the length of time it may be retained, and the manner of its deletion;[89]

Disclosure

- when credit information may be shared electronically;[90]
- any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.[91]

Provisions that speak to privacy include:

Oversight

- *Inspection:* The Act provides for certain circumstances under which records can be inspected. In particular, the Reserve Bank, after authorisation by the central government can inspect all the books and accounts of any credit information company or credit institution.[92]
- *Power to Give Directions*: The Reserve Bank of India has the power to issue directions to Credit Information Companies when it is in public interest, interest of credit institutions, interest of specified users, interest of banking policy, secure proper management of credit information companies, etc.[93]

Access and Correction

- *Personal access*: Any person who applies for a grant or sanction of credit facility, from any credit institution, has the right to request a copy of the information it obtained from the credit information company. Borrowers and clients have the right to ask for their credit information to be updated or corrected at anytime, and the credit institution, company, or specified user must comply within 30 days and only after it has been certified as correct by the credit institution concerned.[94]

Disclosure

- *Disclosure***:** Data that is received by the credit information company is prohibited from

85. Id Section 29.
86. Id. Section 20.
87. *Id.*, section. 19.
88. *Id.*, section. 20(c).
89. *Id.*, section. 20(d).
90. *Id.*, section. 20(e).
91. Id. Section 20(f).
92. *Id.*, section. 12 (1).
93 *Id* Section 11.
94. *Id.*, section. 21(1)(2)(3).

being disclosed to anyone for any purpose, except for its specified user.[95] The only exception to this rule is if it is required by any law in force.

- *Reactive disclosure:* Credit information companies are given the authority, through written notice, to require member credit institutions to furnish information that they deem necessary to comply with the Act.[96]

Offense	Imprisonment	Fine
Person providing false information or omitting to provide information	One Year	Yes. Amount not specified
Credit information company, credit institution or specified user performing any act in breach of the privacy principles	---	Upto Rs. 1,00,00,000/- (Rs. One Crore)
Credit information company, credit institution or specified user providing false information or omitting to provide information	----	Upto Rs. 1,00,00,000/- (Rs. One Crore)
Any contravention of the Act	----	Rs. 1,00,000 and Rs. 5,000 per day if offence is continuing one
• Unauthorised access to credit information is penalised with a fine		Rs. 1 lakh and up to Rs.10,000 for every day that the unauthorised access continues.[97]

Credit Information Companies Regulations, 2006[98]:

In 2006 Regulations under the Credit Information Companies (Regulation) Act were notified. According to the Regulations, Credit Companies are allowed to 1) provide information to individual and corporate borrowers 2) provide data management services to member Credit Institutions 3) collect, process, collate, and disseminate data/information related to investments made in Securities other than those issued by the Central Government.[99] The Regulations define 'data management services' as services which collect, store, devise systems for retrieving, collating, analysing and distributing, publishing, disseminating data, information and other inputs to its members and specified users. [100] Personal data under these Regulations is defined as information about an identifiable individual, but does not include the name, title or business address of telephone number of an employee of the credit information company.[101] The subject of information is defined as one to whom the data,

95. Id. section. 17(4)(a)(b)(c), s. 28.
96. *Id.*, section. 17(1).
97. *Id.*, section. 22.
98 Credit Regulations 2006. Available at: http://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf
99. Id. Regulation 6
100. Id. Regulation 2 (c).
101. Id. Regulation 2 (g).

information, or credit information, relate to and includes a borrower, client, and a person.[102] The principles of privacy are applicable to these Regulations in the following ways:

Oversight

- *Requirement to furnish information:* If a member credit institution is given notice via Form C to provide information back to the Credit information Company, they must do so. [103] Any information that is supplied must be done as specified in Form 'D'.[104]

Disclosure

- *Disclosure of credit report:* Credit Information Companies are allowed to share credit reports only to: a specified user, to comply with a court order, tribunal, law enforcement agency, or statutory/regulatory authority under any applicable law. [105]
- *Proactive disclosure:* The Credit Institutions will ensure updates of the data held by them to credit information companies on monthly (or shorter) intervals.[106]

Access and Correction

- Individuals can request access to credit reports held by Credit Information Companies. [107]

Notice

- Notice of denial of services: If a borrower is denied credit or any other service on the basis of his/her Credit Information Report, the Specified User who has denied credit is obligated to send the borrower a rejection notice within 30 days of the decision stating the specific reasons for rejection along with a copy of the report, the name and address of the Credit Information Company who issued the report, and the information that was used to make the decision.[108] If a borrower requests a report, he/she must pay a fee of Rs.100.[109]

Security

- *Principles:* Credit information companies are to be guided by the following principles. Information collected by the company should be:
  - Accurately recorded, collated, and processed
  - Protected against loss
  - Protected against unauthorized access, use, modification, or disclosure.[110]
  -
- *Confidentiality:* All employees of Credit Information Company's must take a suitable declaration of fidelity and secrecy.[111]
- *Restricted Access:* Credit Institutions and companies must establish procedure for

[102] Regulation 2 (i).
103. Id. Regulation 7.
[104] Id. Regulation 9.1.2 and 7(2).
105. Id. Regulation 9.5.1.
106. Id. Regulation 9.6.3.
107. Id. Regulation 11.
108. Id. Regulation 9.5.5 .
109. Id. Regulation 11 .
[110] Regulation 9.1.1.
[111] Id. Regulation 9.2.2

allowing employees to handle credit information only on a need to know basis.[112]

- *Secure mode of transfer and acceptance:* Credit information must be transferred and received through a secure medium.[113]

Quality/Verification

- *Updation of information:* Credit Institutions are required to update information on a monthly basis and take the necessary steps to ensure that the information is accurate, complete, and current.[114]
- *Accuracy:* The Credit Information Company must make all efforts to ensure accuracy and completeness of data.[115] The Credit Institution is responsible for the correctness and accuracy of the data submitted to the Credit Information Company.[116] Specified users must ensure that they are using latest credit information.[117]

Access and Correction

- *Personal Access:* Individuals have the right to access and obtain a copy of personal credit records after proper identification. Requests for correction of material by a credit institution or specified user must be complied within 15 days by the Credit Information Company.[118]

Collection Limitation

- *Data Collection Limitation:* The data collected must be adequate, relevant, and not excessive, up to date, and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. An example of adequate data collection given in the regulations includes: name, father's name, address, gender, date of birth, contact telephone numbers, PAN, driving license, passport, voter identity card numbers, credit limit, outstanding balance, repayment history, amount and period of default, and primary/collateral security taken.[119]
- *Retention:* Credit Information Companies and Credit Institutions will retain collected and disseminated information for a minimum of seven years.[120] Information relating to a criminal offense will be retained permanently. Information relating to financial default or civil offences will be removed after seven years since the reporting. All information relating to non-individuals will be permanent. [121]
- *Anonymization*: Personal information relating to an individual that is no longer necessary should be destroyed, erased, or made anonymous.[122]

Security

- Protection against misuse: The collector must ensure that collected data is secured

[112] Id. Regulation 9.2.3
[113] Id. Regulation 9.2.5 & 9.2.9
114. Id. Regulation 9.1.3.
115. Id. Regulation 9.6.1.
116. Id. Regulation 9.6.2.
117. Id. Regulation 9.6.4.
118. Id. Regulation 9.3.1, 9.3.2, 9.3.3.
119. Id. Regulation 9.4.1.
120. Id. Regulation 9.7.1 .
121. Id. Regulation 9.7.2 .
122. Id. Regulation 9.7.3.

against loss, unauthorized access, use, modification or disclosure, and misuse.[123]

Disclosure

- Personal data cannot be collected and included in a general publication unless it is collected for a lawful purpose directly related to the function or activity of the credit institution.[124]

Purpose Limitation

- *Use of credit report:* Credit information reports are allowed to be used to: take a credit decisions on various persons, to deter concurrent borrowers and serial defaulters, to keep adverse selection of customers to the minimum, to review and evaluate risk of its customers, to effectively discharge the statutory/ regulatory functions. All other uses are prohibited.[125]
- *Monitoring use:* Credit Information companies will monitor and review on a regular and ongoing basis the access, collection, and usage of a Credit Information Report by the specified user in order to detect and investigate unusual or irregular patterns of use by them.[126]

Notice

- *Notice of Collection:* Before collecting information from individuals credit institutions must ensure that the concerned individual is informed of the purpose of the collection, if the collection is authorised or required under any law and whom the information will be disclosed to.[127] Credit information companies must send notice to member companies when requesting information. This notice is sent in as 'Form C'.[128]
- *Notice of Rejection:* If a borrower is denied credit, the specified user denying the credit must send notice of rejection in writing within 30 days. The notice must state the specific reasons for rejection, include a copy of the credit report, and provide the name and address of any Credit Information Company that issued the report, along with any other information that was used in making the decision.[129]

Accountability

- *Compliance training:* Credit information companies should provide training to employees and establish a compliance committee to oversee the suitability, adequacy of regulations, and create appropriate documentation in relation to their members for furnishing and collecting data.[130]

Openness

- *Privacy Procedures:* Every credit information company must include in their practices and policies information relating to: protection of personal data, acceptance and

123. Id. Regulation 16 (b) (iii) .
124. Id. Regulation 15 (a)
125. Id. Regulation 9.5.3 & 9.5.4.
126. Id. Regulation 9.5.2.
127 Id. Regulation 16(a)
128 Id. Regulation 7.
129 Id. Section 9.5.5
130 Id. Section 18(c) to18(e)

disposal of complaints, security and privacy training, establishing compliance committees, appropriate documentation in relation to their members for furnishing and collecting data.[131]

Penalty/Liability/Redress

- *Liability:* The Credit information company is responsible for the personal data that it is in possession of. This includes data that has been transferred to a third party for processing. The credit information company will use contractual and other means to provide comparable levels of protection while the information is being processed by a third party.[132]
- *Remedies:* An individual may file a written complaint before the Reserve Bank against a credit information company, credit institution, or specified user. The Reserve Bank in turn can place a fine on the company for contravention or may reprimand the company.[133]

The Insurance Regulatory and Development Authority Act, 1999[134]

This Act amended the Insurance Act, 1938, the Life Insurance Corporation Act, 1956, and the General Insurance Business (Nationalisation) Act, 1972.

Oversight

- *Authority:* The Act establishes the Insurance Regulatory and Development Authority to protect the interests of holders of insurance policies and ensure the growth of the insurance industry. Among other things the Authority is responsible for the protection of the interests of policy holders for matters including settlement of insurance claims, nomination by policy holders, and assigning of polices. It is responsible for calling for information, undertaking inspections, conducting enquiries, and auditing insurers. The Authority is also responsible for specifying the form and manner in which books and accounts need to be maintained by insurers, as well as adjudicating disputes between insurers and intermediaries.[135] The Comptroller and Auditor General of India will audit the accounts of the Authority.[136]
- *Advisory Committee*: The Act establishes an Insurance Advisory Committee to advise the Authority on making of regulations and other matters.[137]
- *Furnishing Information:* The Authority has to disclose to the Central Government returns, statements, and other particulars with regard to any proposed or ongoing programme. At the end of nine months the Authority must submit a report on all its activities to the Central Government.[138]
- *Inspection:* The Authority has the power to issue an order in writing for the

131. Id. Section 18 .
132. Id. Section 17.
133 Id. Section 19
134 The Insurance Regulatory and Development Authority Act 1999: http://www.irda.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo108&flag=1&mid=Insurance%20Laws%20etc.%3E%3EActs
135 Section 14.
136 Id. section 17 of the Act
137 Id. section 25 of the Act
138 Id. section 20 of the Act

investigation of the affairs of an insurer. To carry out the investigation the Authority may employ an auditor. Every manager or equivalent director must produce to the Authority all books, accounts, and other documents as required. The Authority may also examine any manager or other officer on oath.[139]

Collection Limitation

- The Authority specifies the minimum categories of information that must be maintained by insurers.[140]

Missing Principles

- Security
- Choice and Consent

Regulations issued by the Insurance Regulatory Development Authority

The IRDA has issued a large number of Regulations to regulate the insurance business in India and keep a vigil on the practices being adopted by insurance companies, agents and brokers, etc. Some of these Regulations also touch upon the privacy of the clients, insurance agents, brokers, etc. A number of these Regulations such as the IRDA (Third Party Administrators) Health Services Regulations, IRDA (Sharing Of Database For Distribution Of Insurance Products) Regulations, IDRA (Insurance Advertisements and Disclosure) Regulations, IRDA Health Insurance Portability Guidelines, IDRA Guidelines on Outsourcing of Activities by Insurance Companies, have already been discussed in the chapter on health privacy. Here we shall discuss some of the other IRDA Regulations which may have an impact on privacy.

Insurance contracts are contracts of indemnity and require that the party being insured truthfully give the insurer all the information necessary for the insurer to enter into the contract and any falsehood in this regard would disable the insured person from claiming the insurance amount. Insurance agents have to explain to the clients the nature of information required in the proposal form and also the importance of such disclosure.[141]

Similarly insurance as well as re-insurance brokers are required to obtain a large amount of information about the clients in order to arrange insurance contracts for them.[142] They are also obligated to provide the IRDA with any information specified by the Authority from time to time within 30 days of requisition.[143] The Authority is also entitled to appoint one or more officers as inspecting authority to undertake the inspection of the premises of the insurance brokers.[144]

Applicants who want to be licensed as insurance agents, actuaries,[145] surveyors or loss assessors,[146] 'specified persons' of corporate agents,[147] insurance brokers, re-insurance

[139] Id. section 33 of the Insurance Act, 1938
[140] Id. section 33(8) of the Insurance Act, 1938
[141] IRDA (Licensing of Insurance Agents) Regulations, 2000, Regulation 8.
[142] IRDA (Insurance Brokers) Regulations, 2000, Regulation 3.
[143] IRDA (Insurance Brokers) Regulations, 2000, Regulation 28.
[144] IRDA (Insurance Brokers) Regulations, 2000, Regulation 29.
[145] IRDA (Appointed Actuary) Regulations, 2000, Regulation 3.
[146] Insurance Surveyors and Loss Assessors (Licensing Professional Requirements and Code of Conduct)

brokers,[148] etc. have to file application forms with the IRDA giving large amounts of personal information in order to obtain their licenses.[149] Similar forms are also required to be filed by such agents, assessors, etc. for renewal of their licenses or registrations.

The IRDA also maintains a register of licensed insurance surveyors and loss assessors with particulars such as their full names, license number and period of validity, professional and other qualifications, areas of survey work, category and any other particulars that the Authority from time to time.[150] The IRDA also has the right to appoint individuals to undertake inspections of survey work, books, records and documents, or investigate a complaint against a surveyor or loss assessor.[151]

The IRDA is also required to maintain the service records of each officer and other employees.[152] The employees also have to inform it about their leave including sick leave, etc. which may contain information which may be too personal to the employee.[153] The employees are also required to give information regarding their movable and immovable properties as well as financial position if the employee is in debt.[154] They even have to inform the Authority if they marry someone who is not an Indian national.[155] Although such information is very pervasive and personal in nature it must be noted that such requirements are quite common for employees working for government departments or other public authorities and are justified in the name of transparency and honesty.

All firms and companies wanting to carry on the business of insurance have to submit a form with a large amount of particulars including details such as names, addresses, occupation, qualifications, experience, etc. of even the shareholders of such a company irrespective of how many shares they hold[156] and the IRDA is entitled to ask for further information in relation to the application.[157] Other than the above, insurance companies are also required to give the Authority various types of information such as the company's finances, assets, investments, auditors' reports, shareholding details, merger schemes, etc. on a regular basis in order to enable the Authority to perform its regulatory and supervisory functions.

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983[158]

This Act places a burden on public financial institutions to maintain the confidentiality of its

---

Regulations, 2000, Regulation 3.
[147] IRDA (Licensing of Corporate Agents) Regulations, Regulation 3.
[148] IRDA (Insurance Brokers) Regulations, 2000, Regulation 6.
[149] IRDA (Licensing of Insurance Agents) Regulations, 2000, Regulation 3(1).
[150] Insurance Surveyors and Loss Assessors (Licensing Professional Requirements and Code of Conduct) Regulations, 2000, Regulation 18.
[151] Insurance Surveyors and Loss Assessors (Licensing Professional Requirements and Code of Conduct) Regulations, 2000, Regulation 20.
[152] IRDA (Conditions of Service) Regulations, 2000, Regulation 8.
[153] IRDA (Conditions of Service) Regulations, 2000, Chapter VI.
[154] IRDA (Conditions of Service) Regulations, 2000, Regulations 44 and 45.
[155] IRDA (Conditions of Service) Regulations, 2000, Regulation 47.
[156] IRDA (Registration of Indian Insurance Companies) Regulations, 2000, Regulations 3 and 10.
[157] IRDA (Registration of Indian Insurance Companies) Regulations, 2000, Regulation 6.
[158] Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983. Available at: http://www.vakilno1.com/bareacts/Laws/The-Public-Financial-Institutions-Obligation-As-To-Fidelity-And-Secrecy-Act-1983.htm

client's transactions. The privacy principles are applicable in the following ways:

Security

- *Secrecy of Data***:** Public financial institutions are prohibited from divulging any information relating to the affairs of its clients except in accordance with laws of practice and usage.[159] To enforce this all banking employees must take an oath of secrecy before carrying out their duties.[160] This obligation of secrecy is also found in the State Bank of India Act.

.

Access and Disclosure

- *Disclosure for discharge of functions*: For the efficient discharge of its functions, public financial institutions may collect from or furnish credit information or other information that it thinks fit to a number of bodies including the Central Government, the State Bank of India, and any other public financial institution.[161]

Payment and Settlement Systems Act, 2007[162]

The Payment and Settlement Systems Act provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India as the authority to oversee connected and related matters. Specifically, the oversight board is known as the Board for Regulation and Supervision of Payment and Settlement Systems. The principles are applicable in the following ways:

Security

- *Confidentiality of Information***:** Any information obtained by the Reserve Bank must be kept confidential.[163] Furthermore, the system provider i.e. any person who operates an authorized payment system, is prohibited from disclosing the existence or contents of any document or any part of any information given to him by a system participant.[164]

Disclosure

- *Lawful Disclosure of Information:* System providers are allowed to disclose information in only three instances: 1. when it is required under the provisions of the Act; 2. if it is expressly consented to by the system participant; or 3. if it is in compliance with orders passed by a court or statutory authority.[165]

Oversight

- *Reactive Disclosure*: When so requested by the Reserve Bank, the system provider is required to provide the Reserve Bank with any information that pertains to the operation of his/her payment system in the form and manner prescribed by the Reserve Bank.[166] The Reserve Bank may ask any system provider for: returns,

159. Id. section. 3(1) .
160. *Id.* Section 4.
[161] Id. Section 3(2)
[162] Payment and Settlement Systems Act 2007. Available at: http://www.lawzonline.com/bareacts/payment-settlement-systems-act/payment-and-settlement-systems-act.html
163. Id. section. 15.
164. Id. section. 22.
165. *Id.*, Section 22(1) .
166. *Id.*, Section 12, 13.

documents, or other information pertaining to its operation of the payment system.[167] The Reserve Bank may also access any information relating to the operation of any payment system and system provider.[168]

- *Inspection*: For the purpose of enforcing compliance with the Act, any officer of the RBI may enter and inspect any premises where a payment system is being operated and may also inspect any equipment, computer system, and documents on the premises.[169]
- *Disclosure:* The Reserve Bank is allowed to disclose information only in four instances: 1. to protect the integrity, effectiveness, and security of the payment system; 2. in the interest of banking or monetary policy; 3. in the course of the operation of the banking system; 4. or in the public interest.[170]

Openness

- *Privacy Policy:* Every client or participant in the system must be made aware of the terms and conditions including charges, limitations, and liabilities under the payment system. Additionally, the clients must be supplied with copies of the rules and regulations governing the operation system etc.[171]

Accountability

- *Audit:* The Reserve Bank may conduct audits and inspections of the payment system or participants.[172]

Penalty/Liability/Redress

Offense	Imprisonment	Fine
Failure to provide information to an officer making an inspection		Upto Rs. 10,00,000 and further Rs. 25,000 per day if the offence continues.[173]
Any person who discloses information without authorization.	Upto 6 months[174]	Upto Rs. 5,00,000 or twice the amount of damages suffered incurred by such act, whichever is higher

The Banking Regulation Act, 1949[175]

The Banking Regulation Act was passed as a means of regulating the Banking industry. The Act empowers the Reserve Bank of India (RBI) to regulate, control, and inspect the banks in India. A Tribunal is also established to investigate complaints made under the Act. Under the Act it is the obligation of the Central Government to set standards for the retention of banking

167. *Id.*, Section 12.
168. *Id.*, Section 13.
169. *Id.*, Section 14 .
170. *Id.*, Section 15(2) .
171. *Id. Section* 21(1) .
172. Id. Section 16.
173. *Id.*, Section 26(3) .
174. Id. Section 26 (4) .

175 Banking Regulation Act, 1949. http://www.pnbindia.in/Upload/En/BANK%20REGULATION%20ACT.pdf

books, accounts, and other documents. [176] The principles are applicable in the following ways:

Oversight

- *Copy of inspection report:* The Reserve Bank is entitled to cause a scrutiny of the affairs of any banking company and its books and accounts. A copy of the inspection report will be provided to the banking company if requested.[177]
- *Disclosure of information in the public interest*: The Reserve Bank and the National Bank for Agricultural and Rural Development, if they deem it to be in the interest of the public, the ability to publish any information obtained under the Act.[178] No banking company can be compelled by any authority to produce or allow the inspection of any books, accounts, documents, or other information that the bank deems to be confidential in nature and whose inspection would result in the disclosure of information relating to any reserves not shown in the published balance sheet, or any particulars not shown in respect with the provisions made for bad and high-risk debts. [179]
- *Inspection:* The Act gives the RBI the authorization to undertake inspection of a bank's books and accounts.[180]
- *Proactive discovery*: The Tribunal constituted under the Act will have the powers of a civil court in certain respects, and among other things have the power of discovery and production of documents.[181] An exception to this standard is that the Tribunal cannot compel the Central Government or the Reserve Bank to produce any books, accounts, or other documents that they claim are confidential in nature, to make any books or documents part of the record of the proceedings of the Tribunal, or to give inspection of any books or documents to any party.[182]

Verification/quality

- *Know Your Customer Norms (KYC)***:** One of the most effective methods of client identification and verification employed by Indian Banks is the Know Your Customer Norms (KYC). The purpose of KYC is to provide a way for banks to ensure that they accept only legitimate customers, accurately identify their customers at each transaction, monitor customers' transactions to detect illegal activities, and implement processes to effectively manage risks posed by customers trying to misuse financial facilities. The norms place the obligation of ensuring the secure and proper management of any banking company on the Reserve Bank. KYC requires:[183] All financial transactions are to be undertaken only after proper identification of the customer. Photocopies of proof of identification should be verified against the original documents. No account may be opened anonymously.
- *Customer Identification Procedure*: Banks must identify the customer and verify his/ her identity by using reliable, independent source documents, data or information. 'The

176. Id. section. 45Y.
177. Banking Regulation Act, 1949. section. 35 (1A)(b) .
178. *Id.*, Section 28 .
179. *Id.*, Section 34A.
180. Id. section 35, Section 45Q.
181. *Id.*, Section 36 AI.
182. *Id.*, Section 36 AI.
183. http://bit.ly/TEiC5i

nature of information/documents required to identify individuals should depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.'

Collection Limitation

- *Requirement to furnish information:* The Reserve Bank may specify and direct a bank to furnish its financial statements and information relating to the business or affairs of any associate enterprise. The Reserve Bank at any time may also inspect the books and accounts any associate enterprise or banking company.[184] Further, every year banks are required to submit a return of the accounts that have not been operated for ten years to the Reserve Bank of India.[185]
- *Data retention:* As a part of the KYC norms, full details of the name and address as well as the details of ID documents should also be kept on record. All transactions (electronic included) should be retained for at least five years. [186]
- *Customer profiles:* Banks are permitted to create customer profiles based on risk categorization that include information pertaining to the customer's identity, social and financial status, nature of business, and customers clients. Banks should only collect information that is relevant and not intrusive. The customer profile cannot be divulged or shared.

Notice

- *Circumstances of beneficiary*: Banks are to clearly establish when customers are permitted to act on behalf of another person/entity.

Security

- *Due Diligence:* Banks must perform 'due diligence' measures based on risk assessment. More intensive due diligence is to be carried out on 'high risk customer's'. These include non-resident customers, high net worth individuals, and trusts, charities, and NGOs.
- *Monitoring of Transactions:* Banks should monitor large or complex transactions and all unusual patterns that do not seem to have an economic or lawful purpose. In order to do this effectively, the bank may prescribe threshold limits for a particular category of accounts and pay particular attention to transactions which exceed these limits. Banks should ensure that a record of transactions in the accounts is preserved and maintained as required by Section 12 of the PML Act 2002.
- *Risk Management:* Banks must adhere to audits, establish internal control systems, circulate lists of terrorist entities, report and identify suspicious transactions, and have

[184] Section 10.
[185] *Id.*, Section 36.
186. http://bit.ly/P1z7Wb

ongoing employee training programmes.

Case law

Shankarlal Agarwalla v. *State Bank of India*,.[187] (1984)
The violation of secrecy and rampant sharing of information between authorities was in evidence again in the case of *Shankarlal Agarwalla* v. *State Bank of India*,.[188] A customer owned 261 bank notes worth INR 1000 each. In 1978, he turned in the notes and asked the bank to credit his current account. The bank disclosed this transaction to the income tax department, which in turn issued a notice under the Income Tax Act. The Calcutta High Court observed that one of the bank's duties to the customer was secrecy. This duty is a duty of contract and not just a moral obligation. Thus, if this duty is breached, an individual could claim damages. The Court however held that the State Bank of India was directed by the Reserve Bank of India and the Ministry of Finance to furnish all particulars regarding deposits of bank notes to the Income Tax Department as soon as such notes were received, thus, this instance was not a violation of secrecy. The Court held as follows:

> "27. Paget on the Law of Banking 9th Edn. P. 166 observed that out of the duties of the banker towards the customer among those duties may be reckoned the duty of secrecy. Such duty is a legal one arising out of the contract, not merely a moral one. Breach of it therefore gives a claim for nominal damages or for substantial damages if injury is resulted from the breach. It is, however, not an absolute duty but qualified subject to certain reasonable if not essential exceptions. The instances are (a) the duty to obey an order under the Banker's Book Evidence Act, (b) cases where a higher duty than the private duty is involved, as where danger to the State or public duty may supersede the duty of the agent to his principal; (c) of a bank issuing a writ claiming payment of an overdraft, stating on the face of it the amount of the overdraft; (d) the familiar case where the customer authorises a reference to his banker.
>
> 28. Under the heading compulsion by law it had been stated that compulsion must be confined to the regular exercise by the proper officer to actual legal power to compel disclosure. It is not every enquiry made by government official which falls within this heading. The learned lawyer appearing on behalf of the petitioner contended that a directive received from the Central Government to disclose the names of the depositors did not fall within that category. Hence disclosure of those informations by the State Bank of India to the appropriate authorities was wrongful. The petitioner contended that the declaration from along with the currency notes for exchange were delivered on the 19th Jan., 1978…… Earlier thereto the State Bank of India was directed by the Reserve Bank of India and the Ministry of Finance to furnish all particulars regarding deposit of bank notes to the I.-T. department as soon as such notice were received. The respondents contended that such communication was made by the respondent 1 in public interest. Under the circumstances, this instant case falls within one of the exceptions as enumerated above…."

[187] AIR 1987, Cal 29. http://www.indiankanoon.org/doc/1300997/
[188] AIR 1987, Cal 29. http://www.indiankanoon.org/doc/1300997/

Case Highlights

- ***Bankers duty of secrecy is not absolute. The instances are (a) the duty to obey an order under the Banker's Book Evidence Act, (b) cases where a higher duty than the private duty is involved, as where danger to the State or public duty may supersede the duty of the agent to his principal; (c) of a bank issuing a writ claiming payment of an overdraft, stating on the face of it the amount of the overdraft; (d) the familiar case where the customer authorises a reference to his banker.***
- ***Disclosure of financial information was made in public interest***
- ***The term privacy is not mentioned***
- ***If a Banker's duty of secrecy is breached, the individual can claim damages***
- ***Due Process still has to be followed when disclosure is made in public interest***

Indian Stamp Act, 1899

The Indian Stamp Act, 1899 is one of the few legislations which most people come in contact with even if they are not lawyers and only dabble in the commercial or even non commercial space. The Indian Stamp Act provides that for a document to be admissible in evidence it must be duly stamped and the requisite stamp duty must have been paid[189] thus making the Stamp Act one of the most important revenue generating legislations for the government. The provisions touching upon privacy are as follows:

Oversight

- *Examination and impounding*. Every person in charge of a public office (including officers entitled to receive documents in evidence) who comes across a document on which stamp duty is payable is empowered to examine the document to determine if proper stamp duty has been paid upon the same and if the duty paid is insufficient such officer is entitled to impound the document.[190]

- *Inspection of Books, etc*. The Collector or any person authorized by him is entitled to inspect any document (and take notes or extracts thereof) in possession of a public officer if such an inspection would lead to the payment of any duty or would prove or lead to the discovery of any fraud or omission in relation to any duty.[191]

Case Law

[189] Indian Stamp Act, 1899, section 35.
[190] Indian Stamp Act, 1899, s. 33.
[191] Indian Stamp Act, 1899, s. 73.

District Registrar and Collector, Hyderabad v. *Canara Bank and others*,[192] (2004)
There was an amendment made to the above provision of inspection in the State of Andhra Pradesh which allowed the person inspecting the documents to also seize and impound the documents. The amendment also extended this power of inspection to include not only public officers but also to citizens and banks.[193] This amendment was applicable only in the State of Andhra Pradesh and was challenged by various people including banks in the case of *District Registrar and Collector, Hyderabad* v. *Canara Bank and others*,[194] because the documents executed between private parties and received and retained in the custody of the bank in ordinary course of their loan advancing transactions were inspected and then the banks were served with a request to pay back the amount of deficit duty on the documents inspected and to recover the same from the parties concerned.

The above amendment in Section 73 was challenged inter alia, on the ground that it intrudes into the privacy and property of individuals. Considering the issue of allowing such inspections at banks which holds the private documents of its customers or copies of such private documents, the question before the Court was whether disclosure of the contents of the documents by the Bank would amount to a breach of confidentiality and would, therefore, be violative of privacy rights of its customers? Discussing this issue the Court held as follows:

> "It cannot be denied that there is an element of confidentiality between a Bank and its customers in relation to the latter's banking transactions. Can the State have

[192] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=26571
[193] The exact text of the amended section 73 (as applicable in Andhra Pradesh) is as follows:
"73 (1) Every public officer or any person having in his custody any registers, books, records, papers, documents or proceedings, the inspection whereof may attend to secure any duty, or to prove or lead to the discovery of any fraud or omission in relation to any duty, shall at all reasonable times permit any person authorized in writing by the Collector to enter upon any premises and to inspect for such purposes the registers, books, records, papers, documents and proceedings, and to take such notes and extracts as he may deem necessary, without fee or charge and if necessary to seize them and impound the same under proper acknowledgement:
Provided that such seizure of any registers, books, records, papers, documents or other proceedings, in the custody of any Bank be made only after a notice of thirty days to make good the deficit stamp duty is given.
Explanation : - For the purposes of this proviso 'bank' means a banking company as defined in section 5 of the Banking Regulation Act, 1949 and includes the State Bank of India, constituted by the State Bank of India Act, 1955 a subsidiary bank as defined in the State Bank of India (Subsidiary Banks) Act, 1959, a corresponding new bank as defined in the Banking Companies (Acquisition and Transfer of Undertaking) Act, 1970 and in the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, a Regional Rural Bank established under the Regional Rural Banks Act, 1976, the Industrial Development Bank of India established under the Industrial Development Bank of India Act, 1964, National Bank for Agriculture and Rural Development established under the National Bank for Agriculture and Rural Development Act, 1981, the Life Insurance Corporation of India established under the Life Insurance Corporation Act, 1956, The Industrial Finance Corporation of India established under the Industrial Finance Corporation Act, 1948, and such other financial or banking institution owned, controlled or managed by a State Government or the Central Government, as may be notified in this behalf by the Government.
(2) Every person having in his custody or maintaining such registers, books, records, papers, documents or proceedings shall, when so required by the officer authorized under sub-section (1), produce them before such officer and at all reasonable times permit such officer to inspect them and take such notes and extracts as he may deem necessary.
(3) If, upon such inspection, the person so authorized is of opinion that any instrument is chargeable with duty and is not duly stamped, he shall require the payment of the proper duty or the amount required to make up the same from the person liable to pay the stamp duty; and in case of default the amount of the duty shall be recovered as an arrear of land revenue."
[194] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=26571

unrestricted access to inspect and seize or make roving inquiries into all Bank records, without any reliable information before it prior to such inspection? Further, can the Collector authorize 'any person' whatsoever to make the inspection, and permit him to take notes or extracts? These questions arise even in relation to the sec.73 and have to be decided in the context of privacy rights of customers...

…Once we have accepted in *Govind* and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-a`-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. If that be the correct view of the law, we cannot accept the line of *Miller* in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory. Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality.

Secondly, the impugned provision in sec. 73 enabling the Collector to authorize 'any person' whatsoever to inspect, to take notes or extracts from the papers in the public office suffers from the vice of excessive delegation as there are no guidelines in the Act and more importantly, the section allows the facts relating to the customer's privacy to reach non-governmental persons and would, on that basis, be an unreasonable encroachment into the customer's rights. This part of the Section 73 permitting delegation to 'any person' suffers from the above serious defects and for that reason is, in our view, unenforceable. The State must clearly define the officers by designation or state that the power can be delegated to officers not below a particular rank in the official hierarchy, as may be designated by the State.

The A.P. amendment permits inspection being carried out by the Collector by having access to the documents which are in private custody i.e. custody other than that of a public officer. It is clear that this provision empowers invasion of the home of the person in whose possession the documents 'tending' to or leading to the various facts stated in sec. 73 are in existence and sec. 73 being one without any safeguards as to probable or reasonable cause or reasonable basis or materials violates the right to privacy both of the house and of the person……..”

Based on the discussion above and other arguments, the Supreme Court of India held the amendment applicable in Andhra Pradesh struck it down.

When the Court says “in the context of a Bank which either holds the private documents of its customers or copies of such private documents, the question arises whether disclosure of the contents of the documents by the Bank would amount to a breach of confidentiality and would, therefore, be violative of privacy rights of its customers?” it seems to suggest that the Court in this case is not really drawing a distinction between the right to privacy of the customer and the bank’s duty to maintain confidentiality.

Case Highlights

- ***Seems to have used the right to privacy and banker's duty of confidentiality interchangeably and not as distinct rights.***
- ***In India, the right to privacy is not referable to the right of 'property' theory.***
- ***Inspection by Collector is an invasion of privacy of both house and person***
- ***The State must clearly define officers by designation or state that powers can be delegated***
- ***Safeguards, including some probable or reasonable cause or reasonable basis or material must be read into provisions related to search, inspection, and seizure. Thus the State cannot make fishing expeditions into the private spaces of individuals.***

Reserve Bank of India Guidelines

RBI Guidelines on Internet Banking, 2011[195]

Due to the ever increasing influence of information technology including the internet and core banking systems the RBI realized that almost every bank was at some stage of technology adoption, be it core banking, mobile banking, ATMs, internet banking, etc. and therefore felt that there was a need to give comprehensive guidance regarding these. It was to address this need that the RBI issued these guidelines to deal with issues relating to information security, electronic banking, technology risk and cyber frauds.

Security:

- *Security Baselines:* Banks should be proactive to identify and specify the minimum security baselines to be adhered to by the service providers to ensure confidentiality and security of data. This is particularly applicable where third party service providers have access to personally identifiable information and critical customer data.

- *Back up records:* A cloud computing system must ensure backup of all its clients' information.

- *Security steps:* An institution may take the following steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated:

    - Address, agree, and document specific responsibilities of the respective parties in outsourcing to ensure adequacy and effectiveness of security practices, including identifying obligations and liability in the event of a breach or default

[195] Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds; http://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf

- Discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need to know basis

- Ensure that service provider employees are adequately aware and informed on the security and privacy policies

- *Confidentiality:* Agreements should provide for maintaining confidentiality of customer's information even after the contract expires or is terminated by either party. Agreements should also mandate controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.

Choice and Consent

- *Default termination:* Contracts between banks and service providers should include conditions for default termination / early exit option for contracts. This may include circumstances when the service provider undergoes a change in ownership, becomes insolvent or goes under liquidation, received judicial indictment (whether within India or any other location), or when there has been a breach of confidentiality, security, or demonstrable deterioration in quality of services rendered.

Security

- *Encryption:* Use of transaction-enabled mobile banking channels requires encryption controls to ensure security of data in transmission. Normally, a minimum of 128-bit SSL encryption is expected. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies.

- *Fraud Risk Management*: It is also necessary that customer confidential information and other data/information available with banks is secured adequately to ensure that fraudsters do not access it to perpetrate fraudulent transactions. Appropriate steps need to be taken to ensure data/information/system security at the Bank. Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes. Appropriate verification procedures should also be incorporated at all channels such as phone banking, ATMs, branches and internet to ensure that only genuine transactions are put through. All the above security measures should be under continuous review for further strengthening. Details in this regard were covered in chapter on information security.

Internet Banking in India – Guidelines 2001[196]

In response to a report issued by a Working Group established by the RBI, the RBI issued guidelines related to technology and security issues, legal issues, and regulatory and

[196] http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0

supervisory issues to be implemented by banks. Although the RBI has also issued comprehensive Guidelines in 2011 (discussed above) it has also clarified that existing guidelines will be an adjunct to the new Guidelines of 2011 unless they are in direct conflict with each other, in which case the Guidelines of 2011 should be followed. The following requirements in the Guidelines of 2001 are relevant to the privacy principles.

Oversight

- *Database administrator:* Banks should designate a network and database administrator.[197]

Security

- *Security Policy*: Banks should establish and put in place an approved security policy. The policy should ensure that there are two groups overseeing the security of banking systems – one to oversee information systems security and one to oversee the implementation of computer systems.[198]
- *Internet requirements:* Banks should ensure that there is no direct connection between the Internet and the banking system, and that real time security alerts are in place.[199]
- *SSL and Encryption:* Banks should use SSL and encryption of at least 128 bit for securing browser to web server communications and encryption of passwords etc.[200]
- *Testing security:* The security of Banking systems should be tested on a regular basis including: attempting to guess passwords, searching for back door traps into systems, attempting to overload the system, checking for holes in software.[201]
- *Logging accesses:* All computer accesses, including messages received should be logged, and banks should use tools to monitor systems and networks for intrusions and attacks.[202]
- *Saving messages:* All applications of banks should have proper record keeping facilities and all received and sent messages should be saved in encrypted and decrypted form.[203]
- *Physical presence of banks:* Only banks that are licensed and have a physical presence in India can offer Internet banking products to residents in India.[204]
- *Confidentiality:* Banks must also maintain secrecy and confidentiality of physical and internet transactions, records, and customer accounts.[205]
- *Access controls:* Banks should introduce logical access controls to banking systems. This could include user-ids, passwords, smart cards, or other biometric technologies.[206]

Verification and Accuracy

- *Identify customers:* Banks must establish and verify the identity of customers.[207]

---

[197] Section (I a.)
[198] Section (I (b))
[199] Section (I(d))
[200] Section (I(f(2)).
[201] Section (I(i))
[202] Section (I(h))
[203] Section (I(l))
[204] Section (III(1))
[205] Section (II(c))
[206] Section (I(c))
[207] Section (II(a))

- *Authenticating Records:* Banks should only use asymmetric crypto system an hash function as a means of authenticating electronic records.[208]

Collection Limitation

- *Backups of data*: All data should be backed up.[209]

Disclosure

- *Outsourcing companies*: Banks should develop guidelines for when information is outsourced.[210]

Notification

- *Notification of security breach:* Banks must report every breach or failure of security systems to the RBI.[211]
- *Notification of risks:* Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template.[212]

Openness

- *Defined contract terms:* The legal basis for transactions will be through bilateral contracts. The rights and obligations of each party must be clearly defined and should be valid in a court of law.[213]
- *Notification of timeframes:* Banks should notify customers of the timeframe and the circumstances in which any stop-payment instructions could be accepted.[214]

Case Law

S. Umashankar vs ICICI Bank, (2010)

In this case, before the Adjudicating Officer under the Information Technology Act, 2010 funds in the amount of INR 6646,000 were suddenly and without authorisation debited from the account of the complainant, S.Umashankar, and posted to another ICICI account. Complaining to the bank resulted only in a promise to look into the matter and reply within a month. A month later the bank replied, describing the loss of funds as a "bank phishing fraud" and, more important, blamed the complainant, saying he had negligently allowed his user name and password to be compromised and failed to follow the bank's instructions regarding fraudulent emails and security controls.[215] The bank also said it could not trace the beneficiary, even though he is an ICICI account holder who had gone through KYC norms verification. The adjudicating officer clearly ruled that the bank failed to establish that due diligence was exercised to prevent unauthorised access as laid out in the data protection provisions of the Information Technology Act. Moreover, the bank also failed to set up security controls with adequate levels of authentication and validation that could have prevented this loss. Further, the officer maintained that there was a definitely a degree of complacency on the part of the bank's officers in dealing with and resolving this issue. The bank was incriminated for lack of due diligence and required to compensate the victim of the fraud.

---

[208] Section (II(b))
[209] Section (I(k))
[210] Section (III(5)(d))
[211] Section (III(5(b)))
[212] Section (III(5)(j))
[213] Section (III(5)(i))
[214] Section (II(d))
215. See http://bit.ly/Ty2pjU

Case Highlights

- ***Banks must practice due diligence to prevent unauthorized access as laid out in the Information Technology Act.***
- ***Banks must establish security controls with adequate levels of authentication and validation to prevent loss.***
- ***Individuals who are victims of fraud have a right to receive compensation for the loss.***
- ***Banks must take responsibility for fraud, even if it takes place with the introduction of new technology.***

Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks, 2013[216]

The RBI issued this Master Circular to provide a framework of rules/regulations/standards/practices to the credit, debit, prepaid card issuing banks and to the credit card issuing NBFCs to ensure that the same are in alignment with the best customer practices. Banks should adopt adequate safeguards and implement the following guidelines in order to ensure that their card operations are run on sound, prudent and customer friendly manner.

Security:

- *Use of Direct Sales Agent (DSAs) / Direct Marketing Agents (DMAs):* When banks /NBFCs outsource the various credit card operations, they have to be extremely careful in the choice of the service provider. In this regard the banks/NBFCs have to be guided by the need to ensure confidentiality of the customer's records, respect customer privacy, and adhere to fair practices in debt collection. **Part I, Para 5.1**

- *Random Checks:* The bank/NBFC should have a system of random checks to ensure that their agents have been properly briefed and trained in order to handle their responsibilities, particularly in the aspects like soliciting customers, hours for calling, privacy of customer information, etc. **Part I, Para 5.3**

Accountability

- *Protection of Customer Rights:* Customer's rights in relation to credit card operations primarily relate to personal privacy, clarity relating to rights and obligations, preservation of customer records, maintaining confidentiality of customer information and fair practices in debt collection. The card issuing bank/NBFC would be responsible as the principal for all acts of omission or commission of their agents. **Part I, Para 6**

Penalty/Liability/Redress

[216] Master Circular on Credit Card Operations of Banks; http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7338

- *Unsolicited Cards and Calls:* Banks should not issue unsolicited cards. In case, an unsolicited card is issued and activated without the written consent of the recipient and the latter is billed for the same, the card issuing bank shall not only reverse the charges forthwith, but also pay a penalty without demur to the recipient amounting to twice the value of the charges reversed. Additionally the aggrieved customer can approach the Banking Ombudsman for further relief. **Part I, Para 6.1(a) and (b)** If unsolicited cards are misused before reaching the customer, any loss arising out of such misuse will be the responsibility of the card issuing bank/NBFC only. **Part I, Para 6.1(c)**

- *Unsolicited loans:* Unsolicited loans or other credit facilities should not be offered to the credit card customers. In case, such a facility is extended and the latter objects to the same, the credit sanctioning bank/NBFC shall not only withdraw the credit limit, but also be liable to pay such penalty as may be considered appropriate. **Part I, Para 6.1(e)**

- *Compliance with TRAI Regulations:* Banks are required to ensure that they only engage telemarketers who comply with the directions and regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time. **Part I, Para 6.1(g)**

Disclosure

- *Limited Disclosure:* The disclosure to the DSAs / recovery agents should also be limited to the extent that will enable them to discharge their duties. Personal information provided by the card holder but not required for recovery purposes should not be released by the card issuing bank/NBFC. **Part I, Para 6.2(d)**

- *Terms for disclosure:* The Master Circular also provides that the terms and conditions which are agreed to by the customer at the time of issuing the credit card should clearly specify the type of information relating to card holder to be disclosed with and without approval of card holder. **Part I, Para 2.5 read with Annex.**

Consent:

- *Consent for disclosure*: The card issuing bank/NBFC should not reveal any information relating to customers obtained at the time of opening the account or issuing the credit card to any other person or organization without obtaining their specific consent. Usually banks, as part of the MITCs, obtain the consent of the customer for sharing the information furnished by him while applying for the credit card, with other agencies. However, the Master Circular specifically provides that banks should give the customer the option to decide whether he is agreeable for the bank sharing her/his information with other agencies. The application form for credit card may be suitably modified to explicitly provide for the same. **Part I, Para 6.2(a)**

Notification:

- *Sharing of information*: Banks need to notify the customer whenever they provide information relating to credit history / repayment record of the card holder to a credit information company in terms of the Credit Information Companies (Regulation) Act, 2005. **Part I, Para 6.2(b)** Before reporting default status of a credit card holder to a Credit Information Company which has obtained Certificate of Registration from RBI and of which the bank / NBFC is a member, banks/NBFCs should ensure that they

adhere to a procedure, duly approved by their Board, including issuing of sufficient notice to such card holder about the intention to report him/ her as defaulter to the Credit Information Company. In all cases, a well laid down procedure should be transparently followed. **Part I, Para 6.2(c)**

Accountability/security:

- *Fair Practices in debt collection:* In regard to appointment of third party agencies for debt collection, it is essential that such agents refrain from action that could damage the integrity and reputation of the bank/NBFC and that they observe strict customer confidentiality. All letters issued by recovery agents must contain the name and address of a responsible senior officer of the card issuing bank whom the customer can contact at his location. **Part I, Para 6.3(b)**

- Banks /NBFCs / their agents should not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude the privacy of the credit card holders' family members, referees and friends, making threatening and anonymous calls or making false and misleading representations. **Part I, Para 6.3(c)**

Master Circular on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2013[217]

The RBI issued the KYC/AML/CFT guidelines to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

Disclosure/Access to Information:

- *Confidentiality:* Information collected from customers for opening accounts is to be kept confidential and not divulged for cross selling or any other such purposes. Banks are also required to ensure that information sought from the customers is relevant to the perceived risk, not intrusive, and in conformity with the guidelines issued in this regard. **Para 2.1(i)**

- *Reporting to Financial Intelligence Unit – India***:** In terms of the PMLA Rules, banks are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND). **Para 2.20(iv)**

- *Cash Transaction Report (CTR):* Banks are required to submit monthly Cash Transaction Reports to the FIU-IND giving details of all individual transactions above Rs. 50,000. **Para 2.22(A)**

- *Suspicious Transaction Reports (STR):* Banks are required to make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences. **Para 2.22(B)(iii)**

[217] Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002; http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7361

Notice:

- *Customer Acceptance Policy (CAP):* Banks are required to lay down clear policies regarding documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time. **Para 2.3(a)(iii)**

- *Customer Identification Procedur*e: Banks are required to lay down a Board approved policy which clearly spells out the Customer Identification Procedure to be carried out at different stages. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in Annex-I to the Master Circular. **Para 2.4(a)**

Collection of Information

- *Customer Profiles:* Banks are required to prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. However, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein cannot be divulged for cross selling or any other purposes. **Para 2.3(b)**

Verification

- *Unique Customer Identification Code (UCIC):* To ensure that customers do not have multiple identities within a bank and across the financial system Banks are advised to introduce a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. **Para 2.4(d)**

Security

- *Mechanisms to Prevent Terrorism related transactions:* Banks are advised to develop suitable mechanisms for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-Ind on priority. **Para 2.13(b)**

Master Circular on Customer Service in Banks, 2013[218]

The RBI, as the regulator of the banking sector, has been actively engaged from the very beginning in the review, examination and evaluation of customer service in banks. It has

[218] Master Circular on Customer Service in Banks;
http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7363

constantly brought into sharp focus the inadequacy in banking services available to the common person and the need to benchmark the current level of service, review the progress periodically, enhance the timeliness and quality, rationalize the processes taking into account technological developments, and suggest appropriate incentives to facilitate change on an ongoing basis through instructions/guidelines such as these.

Disclosure/access to information:

- *Inoperative accounts displayed:* Banks are required to display a list of Inoperative Accounts which are inactive / inoperative for ten years or more on their websites. The list must contain the names of the account holder(s) and his/her address however, the account number, its type and the name of the branch shall not be disclosed on the bank's website. **Para 24.4**

- *Customer Confidentiality Obligations*: The bankers' obligation to maintain secrecy arises out of the contractual relationship between the banker and customer, and as such no information should be divulged to third parties except under circumstances which are well defined. The following exceptions to the said rule are normally accepted:

  (i) Where disclosure is under compulsion of law
  (ii) Where there is duty to the public to disclose
  (iii) Where interest of bank requires disclosure and
  (iv) Where the disclosure is made with the express or implied consent of the customer. **Para 25**

Collection of Information

- *Collecting Information from customers for cross-selling purposes:* The information provided by the customer for KYC compliance while opening an account is confidential and divulging any details thereof for cross selling or any other purpose would be in breach of customer confidentiality obligations. Banks should treat the information collected from the customer for the purpose of opening of account as confidential and not divulge any details thereof for cross selling or any other purposes. Banks may, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Wherever banks desire to collect any information about the customer for a purpose other than KYC requirements, it should not form part of the account opening form. Such information may be collected separately, purely on a voluntary basis, after explaining the objectives to the customer and taking his express approval for the specific uses to which such information could be put. **Para 25.1**

Master Circular on Sharing Information on Wilful Defaulters, 2013[219]

The RBI, to reduce the amount of willful defaults in the financial system the RBI has from time to time come out with various schemes and guidelines such as these.

Access/Disclosure:

[219] Master Circular on Wilful Defaulters; http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7326

- *Access to Borrower's assets:* In cases of project financing, the banks / FIs should ensure end use of funds by, *inter alia*, regular inspection of borrowers' assets charged to the lenders as security; **Para 2.4 (b)**

- *Reporting to RBI / Credit Information Companies:* Banks/FIs should submit the list of suit-filed accounts of wilful defaulters of Rs.25 lakh and above to a duly authorized credit information company of which it is a member. Banks/FIs should also submit the quarterly list of wilful defaulters where suits have not been filed only to RBI. Credit Information Companies thereafter disseminate the information pertaining to suit filed accounts of wilful defaulters on their respective websites. **Para 2.9**

Master Circular on Frauds – Classification and Reporting, 2013[220]

In order to curb of frauds, dacoities, robberies, etc., in banks through better reporting and safety mechanisms the RBI has issued a number of guidelines from time to time such as these.

Disclosure/ Access to Information:
Reporting to RBI and Boards: Banks are required to individually report cases of fraud to the Reserve Bank of India where the cases involve amounts greater than Rs. 1,00,000. Depending upon the amount involved the banks are required to report these cases to different offices of the RBI. **Para 3.1,3.2,3.3**. They are also required to submit quarterly reports of all fraudulent transactions to the RBI, **Para 4** and also report fraudulent transactions amounting to more than Rs. 1,00,000 promptly to their Boards. **Para 5.1.1**.

Reporting to Police: The Reserve Bank has also given specific guidelines to banks for reporting cases of fraud to the police and also specified that in such cases the bank should not be motivated merely by the necessity of recovering the amount but also by public interest and the need to ensure that the guilty persons do not go unpunished. **Para 6**.

Master Circular on Loans and Advances[221]
Banks are encouraged to strengthen their information back-up about the borrowers enjoying credit facilities from multiple banks as under:
(i) At the time of granting fresh facilities, banks may obtain declaration from the borrowers about the credit facilities already enjoyed by them from other banks. These declarations seem to require a large amount of information specific to the borrower which may be of a sensitive nature as is evident from Annex 6 of the Master Circular.
(ii) Subsequently, banks should exchange information about the conduct of the borrowers' accounts with other banks in the format given in Annex 6 at least at quarterly intervals.
(iii) (iv) Make greater use of credit reports available from a credit information company which has obtained Certificate or Registration from RBI and of which the bank is a member. **Paras 2.3.17(a)(i), (ii) and (iv)**

<u>Transfer of borrowal accounts from one bank to another</u>

[220] Master Circular on Frauds – Classification and Reporting;
http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7381
[221] Master Circular- Loans and Advances – Statutory and Other Restrictions;
http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7380

Banks should put in place a Board approved policy with regard to take-over of accounts from another bank. In addition, before taking over an account, the transferee bank should obtain necessary credit information from the transferor bank as per the format prescribed in RBI circular on "Lending under Consortium Arrangement / Multiple Banking Arrangements". This would enable the transferee bank to be fully aware of the irregularities, if any, existing in the borrower's account(s) with the transferor bank. The transferor bank, on receipt of a request from the transferee bank, should share necessary credit information as per the prescribed format at the earliest. **Para 2.4**

B.S.V.S.P. Chaudhary v. *Station House Officer and another*,[222] (2007)

Even the courts of law in India have taken note of the unfair practices sometimes used by banks in debt collection and have repeatedly asked banks to show restraint in such matters. In the case of *B.S.V.S.P. Chaudhary* v. *Station House Officer and another*,[223] the Kerala High Court again warned HDFC Bank regarding the actions of their recovery agents in the following manner:

> "8. Recovery of any amounts due from the customers of the banks should be by a method known to law or a fair practice of debt collection, which has the approval of the Reserve Bank of India, which enjoins the over all supervisory and monitoring power over all the banks in the country. Taking notice of the criticism about the illegal methods being adopted by certain banks issuing credit cards for the recovery of debts due under the credit cards, it appears that the Reserve Bank of India issued certain guidelines to be adopted by all commercial banks issuing credit cards and which are employing recovery agents for collection of dues. It was categorically observed in the guidelines that the banks or the recovery agents should not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude the privacy of the credit card holders' family members, referees and friends, making threatening and anonymous calls or making false and misleading representations. Therefore, the banks or the recovery agents employed by them have to scrupulously follow the guidelines issued by the Reserve Bank of India in the matter from time to time and they cannot resort to the activities of using criminal force against the card holders for recovery of the amounts due. If any such criminal force or harassment is made by the banks or the recovery agents employed by them for due recovery of the amounts due under the credit cards, the affected card holders will have a right to take recourse to law by lodging a complaint with the police or can move the competent Criminal Court having jurisdiction by filing a complaint as required under Sections 190 and 200 of the Code of Criminal Procedure. Whenever such complaints are lodged by credit card holders suffered at the hands of the gundas/recovery agents employed by the banks for recovery of the amounts due to the banks under the credit cards, the concerned police shall register the complaint and after due investigation file necessary reports before the competent court having jurisdiction over the matter."

Case Highlights

- ***Banks and collection agencies cannot use techniques that invade an individuals***

[222] http://www.indiankanoon.org/doc/1450098/
[223] http://www.indiankanoon.org/doc/1450098/

privacy to recover amounts due.

- ***Affected card holders have a right to take recourse to law and lodge a complaint.***

Reports

Damodaran Report on Customer Service, 2010[224]

In response to the growing use and penetration of 24x7 ATMS, Internet banking, debit cards, and mobile banking, in 2010 the RBI established a committee chaired by Shri. M. Damodaran, former chair of the SEBI. The committee was tasked with reviewing the current system of customer service, evaluating grievance redress mechanisms, examining the functioning and effectiveness of the Banking Ombudsman Scheme, looking into new methods of leveraging technology for better customer service and better implementation of safeguards, and reviewing the roles of the directors and regulators. In their report, the committee found many issues with the current system and made recommendations for improvement. Out of these recommendations the following pertain to privacy:

- *Individual Access*: Customers should have the ability to request digitally signed email bank statements. These statements should be accepted by government authorities.
- *Accuracy:* A passbook should be a mirror of the summary of transactions as appearing in the bank's books.

In the case of *Punjab National Bank vs. Rupa Mahajan Pahwa 2008*[225], the Punjab National Bank was charged with issuing a duplicate passbook for a joint savings account to an unauthorised person. The bank was held accountable for the disclosure, and was fined and instructed to look into the conduct of the officials who supplied information to the unauthorised individual. The fact that a bank employee permitted an unauthorised person access to personal information raises the question of whether privacy legislation should require employees in the financial sector to go through training on privacy procedures.

- *Transparency*: If banks are going to suspend an account, they must inform the account holder by SMS. Similarly, banks should inform customers via SMS when an account nears a minimum balance. Banks should also clearly display a list of the most important terms and conditions.
- *Data Bank:* The IBA should establish a KYC Data Bank which can be relied upon for KYC purposes.
- *Identity*: Banks should accept self-attested photographs and proof of address when opening No Frills Accounts. Additionally, all credit and debit cards should contain a photograph of the individual with a scanned signature.
- *Liability:* Customers should be protected and not held liable for loss from ATM/PoS banking transactions.
- *Security*: Banks should put in place fraud detection and prevention systems. These should include giving customers the option of blocking foreign IP addresses and restricting account transfers to specified IP addresses. The committee also suggested

224. Ibid. http://bit.ly/UCabHo
225. See http://164.100.72.12/ncdrcrep/judgement/80PNB%20VS.%20RUPA%20MAHAJAN.htm

that every ATM should be labelled with an ID for use when redressing a grievance. Individuals should be able to easily block their ATM cards via SMS. Cameras should be placed in ATMs so clear pictures can be taken of the individuals using them.
- *Data Retention*: When a complaint is received, banks should preserve any CCTV recordings until the grievance is fully resolved.
- *Redressal*: In the case of fraudulent transactions the lost amount should be credited back to the account. All grievances regarding mobile banking should be addressed by the banks, and not the service providers.

Gopalkrishna Working Group Report, 2011[226]

In April 2011 the RBI's Internet Banking guidelines were reiterated in the G Gopalakrishna Working group on security in E-Banking. The working group created a report advising banks to implement and follow the privacy policies and procedures established by the guidelines. However, the report is meant to enhance the current guidelines to ensure that electronic banking privacy in India is on a par with international standards. Accordingly, the report recommends changes to the current Indian framework to make it more robust. These are meant to set a common minimum standard for all banks to adopt, as well as lay down the best practices for banks to implement in a phased manner for a safer and sounder banking environment. A few of the recommendations include:

- Establish a Chief Information Security Officer;
- Create and implement risk assessments;
- Restrict internal and external access to information to a 'need to know' basis while not impeding regulatory access to data/records and other relevant information;
- Put in place strong data security measures;
- Data transfers should be completed electronically rather than manually to avoid data manipulation. Banks should also have a strong migration policy.
- RBI should still be allowed the right to order inspection of the processing centre, the books, and the accounts.
- Banks should put in place a transaction monitoring and surveillance process to identify irregular transactions.
- ATM cards should be chip based to make it more difficult to steal and reproduce data.
- Boards and senior management of banks should ultimately be responsible for managing outsourced operations.
- Banks must be transparent to the regulator about how much information is outsourced, and the terms and conditions of contracts between banks and service providers should be carefully defined.

Legal suggestions made by the committee include:

- Specify punishments for phishing;
- Put in place and strengthen a legal system to ensure that banks are monitoring transactions in compliance with Anti-Money Laundering legislation;
- Redefine 'electronic cheque' under the Negotiable instruments Act;
- Clarify the term 'intermediary' under the IT Act;
- Clarify whether an individual can be bound by transactions entered into via electronic means;

226. See http://bit.ly/hgjdgt

- Appoint specific agencies to help courts determine the value of electronic records (even if they have not been digitally signed);
- Determine the legal encryption level under the IT Act and establish a committee under section 84A to set rules regulating the use of encryption;
- Ensure that banks are not held criminally and civilly liable for fraud that a customer commits;
- Strengthen the data protection standards found under Sections 43A, 72, and 72A of the IT Act. These recommendations have been met with mixed reviews from the public, For example, critics pointed out that the IT Act already provides punishment for phishing attacks, and many worried about the proposal to exempt banks from liability. Regardless, the report acts as a comprehensive outline to the existing framework for banking in India, and provides a way forward.[227]

Implementation

India, unlike other countries like the United States, does not have specific legislation or a framework regulating and protecting the privacy of financial data. Instead, as pointed out by Mr. Vijayashankar, Cyber Law expert, the confidentiality and secrecy of financial data have evolved as standard practice by banks over the years, and the existing legal protections for financial information have emerged out of anti-fraud provisions. Thus, privacy (specifically data breaches) is not seen as a protected right (while fraud is) and privacy protection for financial information is established predominantly through individual contracts. These practices, though effective in some circumstances, result in inconsistent and incomplete protection for financial data. Additionally, the lack of enforcement leaves a large gap between policy and implementation.

For example, under statute and through policy, banks are responsible for investigating complaints of fraudulent transactions. In practice, however, the onus is almost always placed on the customer. As another example, the KYC norms were developed to detect and prevent money laundering, broadly understood in Indian law as any criminal act that uses the banks as a facilitator. As part of the KYC procedures, banks are required to verify and identify customers, and are responsible for monitoring of their transactions and following up on anything suspicious. In practice, the KYC norms have become a document verification checklist that banks comply with because it's required. Due diligence is rarely given to thoroughly investigating of banking clients, and often the job of following through with the KYC norms is outsourced by banks to another company.

Another weakness of the Indian banking regulatory framework is that the laws have not been amended across the board to take into consideration e-transactions and Internet banking. Therefore, in some cases the same banking regulations that safeguard manual transactions are being extended to electronic ones. This is proving to be inadequate, as privacy risks are higher in the case of electronic transactions. The gaps in the Indian financial regulatory framework have also allowed wide powers of search and seizure to be given to law enforcement and the authorities. Broadly speaking, four bodies have the ability to access financial data. These include the police (but only with case-by-case authorisation), the courts,

227. See http://bit.ly/Ty28NN

the Reserve Bank of India, and the intelligence agencies (where authorisation for specific cases is not required).[228]

The inconsistencies in the implementation and structuring of the financial regulatory framework have left individuals vulnerable to privacy violations of their financial data. In India the most frequently reported privacy violation is banking fraud. The innovative ways in which criminals are accessing and misusing financial information raises the question of whether the current legislation and regulations are adequate to punish and prevent crime. In 2011, the *Economic Times* reported that as many as 11,195 suspicious transaction reports (STRs) were detected by the Finance Ministry's Financial Intelligence Unit (FIU) between 2006 and10.[229] A May 2011 news report revealed that individuals, by working closely with mobile service providers, intercept SMSs that contain the details of financial transactions. These individuals stop any 'alert' SMSs sent from a bank and use a replacement SIM card to send the transaction details to their phone.[230]

Similarly, in June 2011 a scam was discovered in which fraudsters had set up a fake company selling car accessories that offered a discount to buyers who's used a card. When the individuals entered their PINs on handheld devices, the devices copied the card details stored in both the magnetic strip and the PIN. Subsequently, the card details were used to clone the card, and the PIN enabled the withdrawal of money.[231] At present, as discussed above, Indian banks are not taking responsibility for wrongful withdrawals.[232] In another example, in June 2011 six people were able to hack into an account in the ICICI Bank, Chandigarh, and fraudulently sell INR94 lakhs worth of shares in the shareholder's name. Similarly, in May 2012 the RBI issued a public statement warning against fraudulent emails being sent to banking customer's under the auspices of a new security platform being adopted by the bank.[233]

These news items raise questions of liability and effectiveness.[234] In response to these inconsistencies, the Financial Sector Legislative Reforms Commission (FSLRC) is considering a single, harmonised and uniform law applicable to all banks and giving the central bank the power to sanction the takeover of a co-operative bank by commercial banks.[235]

Terms and Conditions from private and public sector:[236]

Private and public sector banks in India implement terms and conditions with implications for their customers' privacy. For example: the private bank ICICI has established a policy that allows the bank to share all information relating to a client's application with other ICICI Group companies, banks, financial institutions, credit bureaus, agencies, statutory bodies, tax authorities, central information bureaus, and other persons as ICICI Bank and its Group

228. Ibid. Interview with NA Vijayashankar
229. See http://bit.ly/QwqFwk
230. See http://bit.ly/iZoziA
231. See http://bit.ly/kDSqWF
232. See http://bit.ly/RM1z10
233. "RBI warns against fraud email", *Economic Times*, May21, 2012, http://bit.ly/P1A6FR20(last accessed on June 16, 2012).
234. http://bit.ly/kvzrdS
235. http://bit.ly/PTOUWh
236. Section research completed by Malavika Chandu intern NUJS law school.

Companies deem necessary or appropriate as may be required for use or processing of the information. Furthermore, under the terms the ICICI Bank and its group companies will not be liable for how that information is used. The terms of this contract are non-negotiable, binary, and changeable at the will of the Bank.[237] These broad terms encompass the relevant banking laws (as discussed in this chapter) and also include any future bodies created by the legislature, under any law. Public sector banks, like the State Bank of India, are regulated by statute and owe a duty of fidelity and secrecy to all their customers. For instance, under the State Bank of India (Subsidiary Banks) Act, 1959 banks must observe, except as otherwise required by law, the practices and usages customary among bankers. In particular, the bank cannot share information pertaining to its clients except in accordance with the law, or when practice and usage customary among bankers deem it necessary or appropriate for that bank to disclose the information.[238] These privacy policies have to comply with all of the laws as discussed above.

Conclusion

- Encryption standards of 128 bit issued by RBI conflict with the 40 bit standards found under the ISP and UASL licenses issued under the Telegraph Act for service providers.
- Lack of standards for information sharing between financial institutions.
- Lack of standards for prohibiting obtaining customer information by false pretences.
- Need for distinguishing between types of financial data collected and shared during transactions.
- Need for requiring comprehensive notices to be given to customers.
- Lack of clear legal redress for individuals. Most frequently individuals must seek redress through courts on a case by case basis.
- Though the RBI Guidelines provide security procedures for financial institutions, many of the legislation pertaining to Finance does not contain adequate security safeguards.
- Lack of harmonized protections for online and offline data

237. See http://bit.ly/P7xRzj: see clauses 18and19
238. State Bank of India (Subsidiary Banks) Act 1959 s. 52.