International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 06-04-2020; Accepted: 08-05-2020; Published: 15-05-2020
www.lawjournals.org
Volume 6; Issue 3; 2020; Page No. 203-206

Confidentiality and data protection in the electronic fund transfer

Rhea Banerjee
4th Year Student, BA.LLB (Hons), Indore Institute of Law, Indore, Madhya Pradesh, India

Abstract
This paper will mainly focus on the electronic fund transfers which can be seen as a developing phase of the banking sector in India. Electronic fund transfers are a kind of alternative method for payment for goods and services and even allows large amount of transactions through EFTs. It can be referred to as bunch of technologies working together for making huge transactions by a safer and faster means without the necessity of having a paper tool of exchange. The basic sections that will be covered in this paper are emergence of electronic fund transfers and its historical origin, modes of electronic banking and kinds of electronic payment. The main part of the paper will be revolving around the privacy and confidentiality issues faced by users while doing electronic fund transfer. Usually transactions where currency is the means of payment, there can be a certain level of anonymity expected but certain details are still required to complete the respective transactions. As per the Electronic Funds Transfer Act of 1978 the EFT terminals and bank statements of EFT banks disclose certain information like date, time etc. In other words, the paper will concentrate on these privacy concerns and how they can be manipulated by the banking institutions while users are making transactions. The author will further advice some suggestions for improving the privacy concerns of EFT systems.

Keywords: electronic fund transfers, confidentiality issues, transactions, banking institutions

1. Introduction
Every banking institution has a set of banking laws, regulations and regulations which are specifically designed to address the fundamental principle regarding safe business practises. To ensure the safety of such businesses, it is important to protect the interests of customers and make sure that they are protected against losses. There are many risks involved in banking business. Some of the common risks with respect to banking sector are fluctuation in market and interest rates, legal risks, liquidity issues etc, and lately with the coming of internet banking there has been an addition to these risks. Even though internet banking has made banking a lot more accessible, but it brings along some major issues like confidentiality of users threatened, illegal electronic fund transfers and others. Internet banking allows huge expansion of this market which is beyond borders and banks try to avoid the problems of regulation and supervision. But here the customers and banks are vulnerable to legal risks like non-compliance with different national laws and procedures, record keeping and report requirements [1].

Due to such existing insecurity, the scope of electronic fund transfers needs to be limited as per the Indian laws and measures should be taken to prevent any kind of further insecurities [2]. In the last three decades, there's been humungous technological advances in the banking sector which has brought about a new issue with regard to electronic fund transfers. EFTs are secure and faster way which are used on a large scale to transfer money round the world. But EFTs come along with certain loopholes such as unauthorized payment risks, credit, insolvency and confidentiality issues [3].

EFT is not so different from the paper-based fund transfers with regard to its regulation. The business world is highly dependent on EFTs for its faster and better procedures. One of the major issues arising out of EFT is consumer protection especially when it comes to defining the liability of loss incurred through these transfers [4]. After the adoption of technology, India has witnessed complete transformation in the banking sector. It has helped the banks to reach to the doorstep of their customers irrespective of their geographical barricades; easing the time, volume and resource restraints. There are structural changes seen in the Indian banking institutions after the 80s when there was a sudden development in the field of Information technology which further led to the introduction of ATMs, E-commerce, etc. Technology is an inseparable tool of present banking sector as it ensures better efficiency, cut down on transaction costs and improves the strategic condition of the banks. Thus, it is essential that Indian banks should implement newer methods of mechanization and communication which affirms a strong and transparent financial infrastructure [5].

1.1 Origin of Electronic Fund Transfer in India
EFT marks its origin when the first ATM was introduced in

[1] Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technonlogy, Vol 5. Issue 4, 3/11/19 11:43 am, https://media.neliti.com/media/publications/28771-EN-electronic-funds-transfer-exploring-the-difficulties-of-security.pdf
[2] Id
[3] Samahir Mohammed Ali Abdulah, Legal Risk Associated with Electronic Funds Transfer, Plymouth Law School, 3/11/19 11:57 am, https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf
[4] Supra 3
[5] Sankalp Jain, Electronic Fund Transfers: A Critical Study in Indian Context with Special Reference to Security & Privacy Issues, SSRN, 3/11/19 12:27 pm, https://papers.ssrn.com/

1960s, and it was capable of handling account transfers, accept deposits, withdrawal of instant cash. EFT was a technical feature which enabled transaction without the use of cash or cheques. The drive of electronic banking was initiated by Reserve Bank of India with the help of various recommendations suggested by different Committees. In 1984, technology was being used in banks to improve their internal working and interaction between branch offices. In 1994, the main aim was to bring about technological advancements in the payment systems, as suggested by Rangarajan Committee Reports in Computerization of Banks. The reports endorsed initiation of EFT system, introduction of MICR clearing for more than 100 banks and marketing concept of card culture. Subsequently in 1995, EFT was launched by RBI with a view to modernize fund transfer in the country and speed up its functioning among the banks [6].

Taking these issues into consideration, the government of India enacted Information Technology Act, 2000 to provide legal recognition to electronic transactions and along with this act an amendment was made to the RBI Act which gave powers to RBI to regulate electronic transfers among the financial institutions [7].

2. Definition of Eft and Its Types

Electronic fund Transfers has not been specifically defined yet, in general sense. Definition of payment given by Goode has been widely accepted all around the world. He defines payment as *"a gift, loan of money or any act offered and accepted in performance of a money obligation."* As per this definition payment should not always be necessarily in form of money and can be in any form of exchange between 2 parties involved in a transaction. With regard to EFT there is no specific definition and it basically aims at replacing paper-based payment orders with electronic methods to authorize a building society, bank or financial institution to credit or debit customer's account. It has been explained that when any machinery facilitates an electronic payment in monetary value while authorizing or granting the payee the right to request the fund transfer from the third party, it permits the payer firstly to escape the transfer of funds in the physical delivery and secondly (where applicable) to obtain a settlement between the payer to the payee' [8].

EFT generally means that movement of an amount of money from customer's bank to another person's bank account by electronic means. EFTs can be classified into 2 main heads, i.e. on consumer basis and on credit/debit transfer basis. Under the consumer category there is further division non-consumer activated EFT which means bank activates the payment which can be a credit transfer or a direct debit, while consumer activated EFT means the customer himself activates the payment, for example by card, these transfers are always described as debit transfers [9].

Non-consumer activated EFT, also known as wholesale EFT means that bank activates the payment through large value transfer system and a consumer activated EFT, also known as retail transaction means the customer activates the payment, which in maximum cases is a debit transfer and usually of smaller amounts initiated by a card, internet payment or via mobile phone. Usually the payment made under consumer activated transaction is transferred immediately from the cardholder's account to the merchant's account, thus every consumer activated EFT is a different contractual agreement governed by separate contracts [10].

Credit transfer is initiated by the payer who order his bank to move funds from his account to the payee's bank account. The payer's bank the moves the amount of transaction in form of any standing order or electronic transfer from his account to the payee's bank account. On receiving the receipt of payment, the amount is debited from payer's account and credited in payee's account. On the contrary, debit transfer can be initiated by both payer or payee. The payee asks his bank to send a request to the bank of payer to send the funds. If the debit transfer is initiated by the payer and passed to payee, for example in case of cheque. Then, the amount of transfer will be credited in the account of payee tentatively and the bank will forward the orders to the payer's bank and eventually the amount will be deducted from payer's bank account. The transfer of funds is considered final when the debit from payer's account becomes irreversible [11].

3. Privacy, Security and Confidentiality Issues Faced Under Eft

Security is one of the major concerns when it comes to electronic transfers. It is very important to protect the honour of EFT transactions or else it will lead to unauthorized or illegal access or use of information of the users. The major problem with electronic transfers is that there is no real evidence as to claim that EFT systems are being hacked at a higher crime rate than paper-based payment system. EFT has got many perks but every system comes along with their own set of loopholes [12]. There are certain vulnerabilities of EFT too, such as

- EFT transactions can lead to unauthorized access to system as customers are directly involved;
- Funds can be removed from the accounts without review of individual by officials dealing with these systems;
- EFT data includes economical value and thus it can be used to destroy the big banks by using the data in form of maliciousness, extortion, terrorism, etc.
- EFT is a crime which is poorly reported as people are not aware about it and there are not satisfactory legislations available for such crime cases and it is not explicitly discussed in the public as it may affect the integrity of the EFT systems and weakening of the reputation of the financial institution [13].

It is one of the main obligations of the payment systems and financial institutions that they should be able to guarantee the safety of assets of their users, to a certain reasonable

[6] Sonia Chawla and Ritu Singhal, "India and the World: The Changing Paradigms in the Banking Sector due to Technological Advancements" Prajnan, Vol. 39, 130 (2010-11), 3/11/19 1:02 pm
[7] Ibid
[8] Supra 3
[9] Ibid
[10] Ibid
[11] Samahir Mohammed Ali Abdulah, Legal Risk Associated with Electronic Funds Transfer, Plymouth Law School, 5/11/19 2:17 pm, https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf
[12] Chp 5, Security in Electronic Fund Transfer, 5/11/19 3:00 pm, https://www.princeton.edu/~ota/disk3/1982/8223/822307.PDF
[13] Id

ground. Assets include not only funds but data also. It should be a protection of data and funds from theft, loss and misuse. Security of such data in important not because the customers are entitled to protection, but they have relied upon the institution that their confidentiality is intact with the system and not readily accessible to anyone. Apart from this, in case there are numerous security failures, then it would signify the poor security of such financial institutions and will definitely weaken the economy of the nation [14].

As per our Indian Constitution, it has been clearly stated that right to privacy is our fundamental right and in cases of EFT transactions, secrecy of the user is very important as the customer is disclosing its personal and financial information to the particular institutions and thus, it is the duty of the bank to ensure that the secrecy and privacy of the customer is maintained. As per Section 43A of the IT Act, 2000, it has been stated that "*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected*" [15].

However, it can be seen that internet Banking has somewhere down the line undermined the fundamental right to privacy of the customers. The protection of information of the customers is mandatory but this information can be disclosed if asked by the law under certain case. As per Section 44(1) of SBI (Acquisition and Transfer of Undertakings) Act, 1980 states, "*The State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information*" [16]. It is the obligation of such banks to protect and maintain the secrecy of their customers unless asked by law or there is some usage customary bankers issue which finds it appropriate to divulge into such information without any expressed consent of the customer.

It has been popularly stated, that one of the primary duties of confidentiality includes non-disclosure of information of their customers acquired by the bank in any manner and it should be guaranteed that such information would be confidential unless it comes under the criteria of public information. The duty of confidentiality is based on an implied contract between the bank and the customer. It is should be understood that liability arises in case of breach of contract and not on basis of insult or damaged feeling of customer. As per the principles of equity, disclosure of information should be done only with the consent of the customer and equity is kept in mind while the information of customer is under protection. The principles of equity also play a major role in deciding the remedy of the injunction to reinforce any contractual duty under such situations [17].

3.1 Eft Crimes in India and Its Reasons

There are many crimes in India which often go unreported as people are not aware of laws, or they want to save their reputation in public, or they are ignorant that something wrong has been done to them. Same is the case with EFT crimes too, EFT crimes generally aim at theft of funds, disruption of data or destruction of the EFT system like there are losses which go unidentified by the account owners as they are of small amount. Another major reason of these crimes is that there are underqualified officers who are not well acquainted with such computer-based frauds and often do not challenge the working of the machinery. The disturbing part of these crimes is that often employee of that particular institution is found guilty for such unauthorised access. They hide such unauthorized procedures and remove it from the computer's memory bank, and unauthorized copying of program and data cannot be easily detected or traced [18].

Some of the common fraud cases under EFT crimes are credit card fraud. In February 2007, 3 people were held guilty in an online credit card scam. Basically, the credit card details of customers were being misused for booking the air-tickets. These offenders were caught by the Cyber Crime Investigation Cell in Pune. It was later found that these offenders were using and manipulating the credit card details of around 100 people and there was a similar case which occurred in Rourkela where police busted a racket of credit card fraud which was of worth Rs 12.5 lakh. The accused hacked into eBay website and made purchases in the name od credit card holders and it was found that they were having the credit card details of about 700 people along with their passwords [19].

There are certain crimes with respect to electronic banking such as Lebanese loop wherein the thief inserts plastic sleeves into the card holder of any ATM, and waits for the user to fall prey to that machine, and as the user moves out thinking that the machine has retained the card, the thief removes the plastic sleeves and inserts the card and respective password and empties his whole account. Similarly, another crime known as "phishing", is a new form of social engineering wherein people are sent fraudulent emails asserting they are from reputable companies in order to entice the customers to give away their financial details like ATM pins, passwords, credit card details etc. The crime rate of phishing has increased in the last few years due to ignorance and unawareness of people [20].

4. Suggestions for Improvement of These Issues

There are plenty of recommendations which can be adopted by our government to improve the current scenario of EFT transactions, like for example the French are experimenting with "intelligent cards" which would be using a microprocessor to access data. Some of the general based

[14] Supra 5, Major issues: Security and Privacy
[15] Section 43A: Compensation for Failure to protect Data, Information Technology, 5/11/19 3:56 pm, https://www.itlaw.in/section-43a-compensation-for-failure-to-protect-data/
[16] Privacy and Banking: Do Indian Banking Standards Provide Enough Privacy Protection?, the Centre for Internet and Society, 5/11/19 4:12 pm, https://cis-india.org/internet-governance/blog/privacy/privacy-banking
[17] Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technology Vol. 5, Issue 4 (2010), 6/11/19 9:33 pm, https://media.neliti.com/media/publications/28771-EN-electronic-funds-transfer-exploring-the-difficulties-of-security.pdf
[18] Supra 5, Major Issues: Security and Privacy
[19] Ibid
[20] Ibid

suggestions to the banking institutions is as follows:

- Customers should be allowed to choose their PIN number in the very first place.
- The institutional computers are generally enclosed and well secured, the access given to employees is limited and their sign-in procedures are recorded. Other than that, they can be protected with monitoring devices and alarms to guard it from any kind of intrusion.
- Better sophisticated protective technologies should be adopted including security against unauthorized insertion of data or instructions and better mechanism for recording the use of programs and modifications made in program.
- One of the best options that banks can opt for is encryption for transmission and storage of data. One kind of encryption is which involves, encoding where coding and decoding is done in public, but actual encryption keys use secret and tight control. Encryption can be used in such a manner that it would not be easy for the common man to decode it or decipher it.
- Further there is an expensive technique measure which can also be adopted where there should be provision for backup of computer processing, data storage, communication lines and power sources [21].
- Lastly, there is an urgent need to implement a new independent body of law to govern EFT transactions. If we have better legislations for such EFT crimes then it would help the customers as well as banking institutions to create an equilibrium between the predictability and certainty of bank's liability of risks associated with EFT. Even the customer would be protected against all forms of unfair contractual terms and conditions [22].

5. Conclusion

It can be concluded that technology is a two-way bridge, if it is providing you means to develop your machinery, then it will definitely have certain loopholes which would lead to some kind of breach in it too. Thus, electronic banking should be applied along with strict legislations and management procedures combined with backup facilities, appropriate Tech officers, physical protection and a significant level of security at cost effective manner. The paper can be further summarized on that one assertion that if people are well aware about the functioning of internet banking privacy and security terms, then it would allow the legislature to bring about new and update legislations which would be at par with the present situation of EFT transactions. As it is very well obvious that current legislations are not adequate for dealing with EFT crimes, and this leads to encouragement among the offenders due to no specific punishments for such crimes. These crimes also lead to weakening of reputation of financial institution and makes them less reliable to their customers. Further, their stability is also at stake and thus establishment of some independent body regarding these issues is necessary to protect and secure the data and funds of our users.

References

1. Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technonlogy, 5(4). 3/11/19 11:43 am, https://media.neliti.com/media/publications/28771-EN-electronic-funds-transfer-exploring-the-difficulties-of-security.pdf
2. Id
3. Samahir Mohammed Ali Abdulah, Legal Risk Associated with Electronic Funds Transfer, Plymouth Law School, 3/11/19 11:57 am, https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf
4. Supra 3
5. Sankalp Jain, Electronic Fund Transfers: A Critical Study in Indian Context with Special Reference to Security & Privacy Issues, SSRN, 3/11/19 12:27 pm, https://papers.ssrn.com/
6. Sonia Chawla and Ritu Singhal, "India and the World: The Changing Paradigms in the Banking Sector due to Technological Advancements" Prajnan, Vol. 39, 130 (2010-11), 3/11/19 1:02 pm
7. Ibid
8. Supra 3
9. Ibid
10. Ibid
11. Samahir Mohammed Ali Abdulah, Legal Risk Associated with Electronic Funds Transfer, Plymouth Law School, 5/11/19 2:17 pm, https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf
12. Chp 5, Security in Electronic Fund Transfer, 5/11/19 3:00 pm, https://www.princeton.edu/~ota/disk3/1982/8223/822307.PDF
13. Id
14. Supra 5, Major issues: Security and Privacy
15. Section 43A: Compensation for Failure to protect Data, Information Technology, 5/11/19 3:56 pm, https://www.itlaw.in/section-43a-compensation-for-failure-to-protect-data/
16. Privacy and Banking: Do Indian Banking Standards Provide Enough Privacy Protection?, the Centre for Internet and Society, 5/11/19 4:12 pm, https://cis-india.org/internet-governance/blog/privacy/privacy-banking
17. Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technology, 2010, 5(4). 6/11/19 9:33 pm, https://media.neliti.com/media/publications/28771-EN-electronic-funds-transfer-exploring-the-difficulties-of-security.pdf
18. Supra 5, Major Issues: Security and Privacy
19. Ibid
20. Ibid
21. Supra 12, Technology and Techniques for increased EFT Security
22. Supra 3, Recommendations

[21] Supra 12, Technology and Techniques for increased EFT Security
[22] Supra 3, Recommendations