Crimes and Security in E-Banking

Annirudh Vashishtha[1]
Dr. Vijendra Singh[2]

Abstract:

Banks are an important institution of the economy for providing institutional credit to its customers. A banking company in India is the one adding from the public, repayable on demand or otherwise and withdrawal by cheques, draft, order or otherwise. In simple terms, a bank accepts money on deposits, repayable on demand and also earns a margin of profit by lending money. A bank stimulates economic activity in the market by dealing in money. It mobilises the savings of people and makes funds available to business financing their capital and revenue expenditure. It also deals in financial instruments and provides financial services for a price i.e, interest, discount, commission, etc

The growth of internet and e-commerce is dramatically changing in everyday life, with the world wide web and e-commerce transforming the world into a digital global village. The latest wave in information technology is internet banking. It is a part of virtual banking and another delivery channel for customers.

In simple terms, internet banking means any user with a PC and a browser can get connected to the banks website to perform any of the virtual banking functions and avail of any of the bank's services. There is no human operator to respond to the needs of the customer. The bank has a centralised data base that is web-enabled. All the services that the bank has permitted on the internet are displayed on a menu. Any service can be selected and further interaction is dictated by the nature of service. The range of services offered by e-banking are: Electronic Funds Transfer (EFT0: Automated Teller Machines (ATM) and point of sales (PoS), Electronic Data Interchange (EDI) and Credit Electronic or Digital cash.

What is addressed generally with regard to E-Commerce under the title of safety of communication and data protection is a specific problem of banking law since bank secrecy is one of the most crucial and important problems of bank business. This is more or less true for all countries. Therefore, the question arises how the requirements of protecting of bank secrecy can be complied with in electronic transactions.

Problems of Jurisdiction

With the present case of communications and the shrinking of the global marketplace, an accurate determination of the appropriate jurisdiction of a particular transaction becomes increasingly important. Furthermore, as a result of the unprecedented pervasiveness of the Internet as a medium, the intentional violation of Transboarder laws has become a common occurrence. Consequently, the redressal of these grievances before the nearest judicial forum, has sparked off the evolution of a new brand of jurisdictional jurisprudence with startling results. Since there is little or no domestic legislative recognition of the need to evolve a distinct set of regulations for internet jurisdiction, the decisions of various courts of the United States as well as the European Courts, are the only guide to the issues relating to the jurisdiction of courts over the internet.

So the paper shall try to study various services offered and crimes committed in E-banking and also how can a customer be protected, a special reference shall be given to the problem of jurisdiction under E-Banking.

Keywords: *E-commerce, World wide web, Transborder laws, Jurisdictional Jurisprudence, Pervasiveness*

I. INTRODUCTION

Banks are an important institution of the economy for providing institutional credit to its customers. A banking company in India is the one adding from the public, repayable on demand or otherwise and withdrawal by cheques, draft, order or otherwise. In simple terms, a bank accepts money on deposits, repayable on demand and also earns a margin of profit by lending money. A bank stimulates economic activity in the market by dealing in money. It mobilises the savings of people and makes funds available to business financing their capital and revenue expenditure. It also deals in financial instruments and provides financial services for a price i.e, interest, discount, commission, etc.

II. E-BANKING

The growth of internet and e-commerce is dramatically changing in everyday life, with the world wide web and e-commerce transforming the world into a digital global village. The latest wave in information technology is internet banking. It is a part of virtual banking and another delivery channel for customers.

In simple terms, internet banking means any user with a PC and a browser can get connected to the banks website to perform any of the virtual banking functions and avail of any of the bank's services. There is no human operator to respond to the needs of the customer. The bank has a centralised data base that is web-enabled. All the services that the bank has

[1] Amity Law School, Amity University, Noida
[2] Amity Law School, Amity University, Noida

permitted on the internet are displayed on a menu. Any service can be selected and further interaction is dictated by the nature of service.

In this new digital market place banks and financial institutions have started providing services over the internet. These types of services provided by the banks on the internet called e-banking. E-Banking lowers the transaction cost, adds value to the banking relationship and empowers customers, e-banking is electronic banking or banking using electronic media. Thus, e-banking is a service provided by many banks, that allows, a customer to conduct banking transaction, such as managing savings. Checking accounts, applying for loans or paying bills over the internet using a personal computer, mobile telephone or handheld computer (personal digital assistant) The range of services offered by e-banking are: Electronic Funds Transfer (EFT0: Automated Teller Machines (ATM) and point of sales (PoS), Electronic Data Interchange (EDI) and Credit Electronic or Digital cash.

III. BENEFITS

There are various benefits of e-banking provided to customers which are:

E-banking provides 24 hours, 365 days a year services to the customers of the bank: Customers can make some of the permitted transactions from office or house or while to a modern traveling via mobile. The benefits are: e-banking provides unlimited network to the bank and is not limited to the number branches. Any PC connected to a modern having an internet connection can provide cash withdrawal needs of the customer. Load on branches can be considerably reduced by establishing centralized data base and by taking over some of the accounting functions.

IV. CRIMES IN E-BANKING AND PROBLEM OF JURISDICTION

Crimes in E-Banking

With the rapid advancement in the technology over the years, our vulnerability has increased with the perceived value of and reliance on this technology. Any big organization in the world today uses computers to conduct its business. Computers compile, generate and store data and are the lifeblood of any sizeable business in the world today. Companies need information everyday, information about raw materials, stock markets, management of accounts etc. With the huge advancement in technology over recent years, data theft is the new 'invisible' crime, and poses a real threat to banks and businesses alike. It is a 'faceless' crime, which makes it extremely appealing to those criminals with the technical know-how. Businesses which hold a lot of sensitive public and personal details should be even more careful with the information they hold.[1]

V. DATA FRAUD

Fraud, pure and simple isn't a crime; rather there are very few elements in the criminal law, which use the word 'fraud' directly. The definition of data fraud has been altered from time to time to incorporate the various offenses that emerge as a consequence of escalation in cyber technology. The Council of Europe defines data fraud as …"the input, alteration, erasure or suppression of computer data or computer programmes , or other inferences with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property to another person with intent of procuring an unlawful economic gain for himself or for another person."

VI. A-Z OF DATA FRAUD

Data fraud in itself comprises of a whole subset of various misdeeds. There are various crimes that fall within the ambit of data fraud. Some of the prominent ones are:

- **Internet Banking Fraud**

  During the past decade, the growth of internet has increased exponentially with various workhouses being equipped with sophisticated technologies to boost their efficiency levels to an optimum. The concept of internet banking was introduced to facilitate the depositors to have access to their financial undertakings globally. But every good thing has its own demerits; the introduction of this system was coupled by a number of fraud incidents in which the money of depositors was embezzled by the net swindlers popularly known as hackers.

  The great advantage of using the Internet for bank robberies is that it works beyond borders. I can sit in Nigeria, or the Philippines, and pilfer a bank account in the Netherlands, or the Scottish highlands. The Dutch victim will contact whom? First his bank. They can't trace the money, or they only can to a certain point. They can't trace it if it has been channeled into the e-gold.com system.

- **Digital Extortion**

  For any company doing business on the Internet, it's the sound of doom: a computer voice warning of an inbound attack. Call it a cyber-shakedown: A hacker threatens to shut down a company's Web page, unless the business pays up. Not only this, a much threatening could be the disclosure of company's secret data to its rivals. Digital Extortion can be defined as, "Illegally penetrating through the system of an enterprise and then compelling it to pay substantial amounts in lieu of their secret data or to save their system from being wiped out by the hackers."

- **Credit Card Frauds**

  Credit Card popularly known as plastic money has came up as a panacea for the troubles of carrying huge amount of money in the pocket. The credit card embodies two essential aspects of the basic banking functions: the transmission of payments and the granting of credit. But again the usage of this technology has brought in new forms of crimes with the fraudsters employing entirely new technologies to manipulate this technology for their illegal economic gains.

[1]Wiegand Wolfgang, "Legal aspects of Banker Customer relationship in E-Banking", Kluwer Law International, Netherlands, 2002.

Types of Frauds:

The fraud can be simple but ingenious, it can be technologically advanced, it can be of a type which can be perpetrated by a single person or a group of people. Every time the card issuers come up with a new security measure, the fraudster comes up with something to counter that security measure. The credit card frauds can be classified into various types:

- **Cyber Trespass**[2]

  In common language the word 'trespass', means to go on another's property without consent. Though it is ordinarily a civil wrong, if trespass is done with criminal intention, it is treated as criminal trespass. Thus, as trespass actions are stranded in the idea of protecting an owner's control over his property and as even the websites should be considered as a species of property. As like in the case of tresspass, when just cracking is there by the cracker, it is of a civil nature but once the intention to cause harm or rather damage the system is proved, the liability becomes that of a penal nature. Now it is not just criminal tresspass, which can be done by cracking but cracking may also result in many other crimes which are mentioned in the Indian Penal Code, 1860. Like, if a cracker cracks a banking website and transfers money into his own account, this may constitute a crime under Sec.378 of the Penal Code, which in this case may also be termed as cyber Theft. The IT Act tries to achieve this by providing civil and penal consequences for cracking and other wrongful activities. The development of new-age technology in the form of computers and other such instruments is the cause of rampant tort of cyber-trespass.

VII. PROBLEM OF JURISDICTION

Under traditional legal systems, the transactions between parties when both are situated in distinct territorial jurisdictions, are governed either by the laws of the country which the parties agree will govern the transaction, or by the laws of the country in which the transaction is performed. These traditional notions of jurisdiction have no relevance to the activities carried out over the Internet is insensitive to the activities carried out over the Internet, as the Internet is insensitive to vocational constraints. The nature of the Internet is such, has to allow persons from geographically distinct locations (and jurisdiction) to transact with each other, with little or no comprehension of the consequences of their actions in the jurisdiction within which they are operating. In fact, the absence of geographical limitations (that normally indicate the applicability of a different set of laws to the enforcement of a contract) could lead the incautious to believe that the laws of their home state apply to their actions, when in fact they are in inadvertent violation of the laws of another state.

In these circumstances, the courts could, and do, assume jurisdiction over the offence and try the offender within their own jurisdictions, resulting in situations where persons located in a completely different jurisdiction may be tried in a court of a given territory. There have been various examples of foreign courts assuming jurisdiction over a matter that *prima facie* arose in a different jurisdiction, on the strength of the long arm statues of that state.[3]

- **Indian Context**

The Indian jurisprudence with regard to jurisdiction over the Internet is almost non-existent. In the first place, as the result of the strongly unitary model of Government prevalent in India, interstate disputes never assume the level of private international law. Hence, their has been precious little by way of development of private international law rules in India. Furthermore, there have been few cases in the Indian courts where the need for the Indian courts to assume jurisdiction over a foreign subject has arisen. Such jurisprudential development would however, become essential in the future, as the Internet sets out to shrink borders and merge geographical and territorial restrictions on jurisdiction.

It is worthwhile to consider the issue of jurisdiction at two levels. In the first place, given the manner in which foreign courts assume jurisdiction over the Internet related issues (as evidenced by the cases discussed above), the consequences of a decree passed by a foreign court against an Indian citizen must be examined. In other words, under what circumstance can the decision of a foreign court be enforced against an Indian citizen or a person resident in India. It is also necessary to examine the circumstance under which the Indian courts would assume jurisdiction over foreign citizens in order to better understand the rights of an Indian citizen who is affected by the act of a foreign citizen.

VIII. CONCLUSION

Though the law of consumer protection is strong in India, remedies have ceased to be effective because of delay in consumer courts. Moreover, manufacturers, traders and service-providers have found ways and means to defeat the right of consumers by introducing limited-liability clauses in contracts with consumers. Such clauses are upheld as legal because consumers accept them. The onus therefore lies upon the consumers to protect their own rights.

Cyber consumerism is likely to provide the greatest law of consumer protection, i.e, fierce global competition where survival of manufactures, traders and service-providers would depend upon quality of goods and services and not upon standard form of contracts, which are devious, one-head, heavily loaded in favour of manufacturers and traders and adverse to consumersition.

IX. INTRENET SECURITY

For the purposes of business document exchange via EDI, end-to-end security mechanisms are crucial and have to be implemented. In the larger context of Electronic Commerce, it is extremely important to secure internal information systems from being attacked from outside. With client machines on an organisation's internal LAN routinely accessing the Internet, they become targets for attack by unscrupulous elements.

[2]Dr. Tabrez Ahmad, Dimensions of Cyber Tresspass in India, KI IT Law School, KIIT University. August 24, 2009.
[3]Matthan Rahul, The Law relating to Computers and the Internet, Butterworths India, New Delhi.

Firewalls which are built to protect the internal network of an organization from attacks originating from the Internet should be implemented in many ways. Some of those ways are:

- Establishing rules to decide which packets, depending on the originating IP address should be allowed to pass into the organisation's network.
- Establishment of proxy servers, so that internal client requests for accessing external services are routed through the proxy server. This ensures that the client and the external server are not in direct communication with each other.
- Establishment of an additional network as a buffer between the internal and external networks.

Web communication also requires additional levels of security to protect against situations such as compromise of credit-card numbers when transmitted across the network.

X. BIBLIOGRAPHY

1. Mark Hapgood *QC, Paget's Law of Banking,* Thirteenth Edition, Lexis Nexis Buttterworths.
2. Tannan M.L.,*Tannan's Banking law and practice in India*, Twenty First Edition, Wadhwa Nagpur, 2005.
3. Kamath Nandan, *Law relating to Computer Internet & E-Commerce,* Third Edition, Universal Law Publishing Co., 2007.
4. Verma S.K. & Mittal Raman, *Legal Dimensions of Cyberspace,* Indian Law Institute ,2004.
5. K. Bajaj Kamlesh and Nag Debjani, *E-Commerce- The cutting Edge of Business*, Tata McGraw-Hill Publishing Co. Ltd., New Delhi.
6. Chissick Michael and Kelman Alistair, Electronic *Commerce Law and Practice*, Second Edition, London Sweet & Maxwell 2000.
7. Matthan Rahul, *The Law relating to Computers and the Internet*, Butterworths India, New Delhi.
8. Wiegand Wolfgang, "Legal aspects of Banker Customer relationship in E-Banking", Kluwer Law International, Netherlands, 2002.
9. Sood Vivek, Cyber Law Simplified, Tata McGraw-Hill Publishing Co. Ltd., New Delhi.