6.1 Introduction

Information technology has dramatically altered the way in which financial services are delivered to consumers. This chapter outlines the origin of ‘e-Banking’ and its impact on e-Commerce transactions. e-Commerce is an economic solvent as it dissolves old business models, changes the cost structure and re-arranges links among buyers, sellers and everyone in between. e-Commerce is a potent socio-economic chemical that reacts with everything it touches; Indian financial structure, in general, and Indian Banking system, in particular. The fundamental focus of this chapter is on the threats to consumers in an online shopping, particularly at the moment, when they make payment through online banking or Internet banking. For the purpose of this chapter, electronic banking is considered to be the retail banking. Retail banking is banking in which banking institutions execute transactions directly with consumers, rather than corporations or other banks. It sketches mainly the frauds to consumers in an online world as any contract or commercial transaction is invalid without movement of money (consideration) and reveals that how this movement of money via e-Commerce mode of payments has become haven for cheaters or criminals.

“Ever since men began to modify their lives by using technology they have found themselves in a series of technological traps.”

Reger Revelle

Advancement in technology has revolutionized today’s landscape. Technological advancements have brought this generation to a situation where everything is moving at a great pace.¹ The last decade in the global arena has witnessed a drastic and tremendous growth in the field of Information Technology wherein world has turned

---
from postal to portal world. In the era of Information Technology no business can afford to remain on the sidelines. Technological change comes in waves, and just as the ocean erodes the shores so too technology erodes the traditional strategies causing business models to behave in different ways. e-Commerce is an economic solvent. It dissolves old business models, changes the cost structures, and re-arranges links among buyers, sellers and everyone in between. In nutshell, e-Commerce is a chemical that reacts with everything it touches. e-Commerce is to the information revolution what the railroad was to the industrial revolution and like the railroad; e-Commerce has created a new and charismatic boom by rapidly changing the economy, society and every segment of society. Indian financial economy is passing through an unprecedented phase of an unparallel metamorphosis in the arena of ‘e’ technology and ‘e-Commerce’. The most outstanding development in e-commercial transaction has been the geometric expansion of ‘Online Banking’ or ‘e-Banking’. Going “e” is a central act that shapes every subsequent plan and decision a company makes. e-Commerce is a three-legged stool. If one company has two of the legs namely-(1) Infrastructure (Speed), (2) Valid contractual Software, but don’t have the very important one and that is (3) e-Banking facilities (price or consideration or effective e-transaction services), there is no way that stool will ever stand up. Therefore, the growth of e-Banking has an integral role in the establishment of e-Commerce and online shopping.

In the 21st century online banking or e-Banking has made inroads in the lives of every walk of human life. In the present scenario, the business world is surrounded by

---

5 ibid., pp. 20-21.
6 ibid., p. 20.
benefits of ‘e-Banking.’ e-Commerce has become a global reality. It encompasses four stages in a valid sale or purchase during online shopping namely: (i) e-Commerce Infrastructure of company, (2) Internet facility with consumers, (3) Valid contract (offer, acceptance, consideration or movement of consideration) and (4) Money (e-Banking). The payment of money in an online shopping acts as one leg of the e-commercial transactions.  

“Now a days, half of trillion dollars change hands everyday although no hands are involved, and in a sense, no dollars either, and it’s not even numbers really. It’s just binary sequences of pulses racing between computers.”

Robert Krulwich

Prior to embarking on a journey on the information highway, if a consumer wishes or intends to transact in cyberspace, it is necessary to be equipped with a mode of payment. The Internet facility might be free, but the goods and services available come at a price. The method of payment in cyberspace, wherein Internet and e-Commerce has taken a leading role in commerce has undergone a significant change. The majority of online Business-to-Consumer transactions are currently influenced by new modes of e-payment. The business environment in which a banker functions in India now stands attuned to the present global environment. Internet banking acts as a vehicle that delivers most of our banking needs to us right where we are. This vehicle brings to our doorstep almost all of the banking facilities.

Retail banking in India has fast emerged as one of the major drivers of the overall banking industry and has witnessed enormous growth in the recent past. Retail

---

11 Kiron Prabhakar, “Payment Mechanism on Cyberspace” in S.B. Verma and Raman Mittal (edited), Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, 2004, pp. 96-112 at p. 96.
banking is banking in which banking institutions execute transactions directly with consumers, rather than corporations or other banks. Services offered include savings and transactional accounts, mortgages, personal loans, debit cards and credit cards.

Retail Banking is a quick enormous market banking where individual customer can use numerous branches of the commercial banks which are interconnected. Banks provide savings accounts, current accounts, checking accounts, personal accounts, tax exemption special savings accounts, time deposit accounts, money market accounts, loan accounts and joint accounts, variety of mortgages, different types of loans and different types of customer automated teller machine services. Now-a-days the customers are using all these facilities in day to day life. There are two important components of retails banking services namely: (a) Retail Liability Products and (b) Retail Assets Products. The retail banking environment is changing very fast. Therefore, it is required to look into risks and solutions involved in customer security management in retail banking. This chapter highlights various risks to consumers in retail banking.

6.2 Changing facets of Payment Mechanism: From Commodity Money to Plastic Money

Payment in its most primitive form involves barter; the direct exchange of goods and services for other goods and services. This barter form of payment suffers from the need to establish what is known as a double coincidence of wants. Consequently, over the centuries, barter arrangements have been replaced with other forms of money. The earliest form of money was called commodity money; where physical commodities such as corn, salt or gold whose values were well known were used to effect payment. In order to acquire desirable properties, gold and silver became the most commonly used commodity money, particularly after the industrial revolution in the 1980s. In the

---

14 Retail Liability Products: Any amount owed by bank by accepting the various deposits from an individual for a fixed period of time. It includes mutual funds, bonds, tax-free relief bonds, fixed deposits and saving accounts etc.

15 Retail Assets Products: The retail asset products are small offering. These offerings are loans or advances given to individual e.g. commercial vehicle loans, customer durable loans, housing loans against property, education loans etc.

16 Double Coincidence of Wants: This means, for example, that a person wishing to exchange food for a bicycle must first find another person who is both hungry and has a spare bicycle.
progression of money, there came the use of tokens such as paper notes, which were backed by deposits of gold and silver held by note issuer. This was referred to adopting a commodity standard as economy became highly stable and government was trusted, therefore, it was unnecessary to have commodity backed by notes. Therefore, cash payment became one of the most popular forms of money transfer.\textsuperscript{17}

In India or anywhere in the world, the backbone of any financial institution is ‘Money.’ Banking industry is one of the oldest industries in the world\textsuperscript{18} and money runs like blood in the body of financial institutions.

\begin{quote}
\textit{“Money is like a sixth sense- and you can’t make use of the other five without it.”}
\end{quote}

\textbf{William Somerset Maugham}

Money has been around in one form or the other with various characteristics. Since almost 5000 B.C. numerous materials (coin or paper notes) have been used for money because it performs so many functions in society. When exchange was the only rule of market, barter system flourished wherein a carpenter could exchange a chair or table for a sackful of grains. When store of value was an additional function demanded of money, coins and notes emerged, bringing with them increased trade, banks and other financial institutions. There are various functions of money like-(i) Money is a medium of exchange, (ii) It is a measure of value, (iii) It is a store of value and (iv) It is a standard of deferred payment. Money has evolved over thousands of years to attain new characteristics and to perform new functions. Apart from these reasons, money has certain other features because of which it has evolved, namely: (i) Money is a legal tender, (ii) It is easily recognizable, (iii) It’s value can be calculated easily, (iv) It


\textsuperscript{18} Banking Industry: The banking industry in India has a huge canvas of history, which covers the traditional banking practices from the time of Britishers to the reforms period, nationalization to privatization of banks and now increasing numbers of foreign banks in India. Therefore, Banking in India has been through a long journey. Banking industry in India has also achieved a new height with the changing times. The use of technology has brought a revolution in the working style of the banks. Nevertheless, the fundamental aspects of banking i.e. trust and the confidence of the people on the institution remain the same. Quoted from: K.A. Goyal and Vijay Joshi, “Indian Banking Industry: Challenges and Opportunities”, \textit{International Journal of Business Research and Management (IJBRM)}, Volume 3, Issue 1, 2012, p. 18.
facilitates buying without being transferred into any other form and (v) it is acceptable to society.\textsuperscript{19}

One of the very oldest dimensions of money is coin. Coins are easy to carry around and useful for small value purchases. Coins are generally left alone by counterfeit and are also not easily mutilated.\textsuperscript{20} Paper currency which is printed in large denominations as well as small is useful for large value purchases. Paper currency can be stored in much smaller place than coins. Even today money is evolving. A shift has been introduced in the trend relating to currency- from paper currency to plastic currency. In fact, the 20\textsuperscript{th} century has seen changes in forms of money like never before. Today, plastic payments are common to most developed nations and are gaining ground in developing and to some extent in underdeveloped countries too. Plastic cards are touted as “tomorrow” payment systems. The present generation is supposed to be moving towards a cashless society-where most of the payments and purchases are done by plastic money.\textsuperscript{21}

Plastic cards have all the advantages of coin and paper currency. It also has an added function of identification. Since the plastic card have a signature panel (photograph of the card-holder), the acceptor of the card can verify if the holder is the legitimate holder of the plastic card.\textsuperscript{22} Plastic cards also keep track of transactions as they are incurred along with all details of the purchases such as the shop name, date of purchase, amount of purchase, city of purchase etc., etc. A major drawback of plastic cards as payment mode is its heavy dependence on technology like satellites, phone line, computer links, LANs, WANs and Internet etc. A snag in any one of these can cause a major disruption in acceptance procedures.\textsuperscript{23} The development of ‘plastic money’ is probably the most relevant phenomenon of the modern banking era. Plastic money comes in various forms


\textsuperscript{21} Rupa Mehta and Rohinton Mehta, 2009, pp. 1-4.

\textsuperscript{22} If paper money is stolen from A and used by B in X’s shop, X has no way of knowing that the money is stolen. If as A’s card is stolen and used by B in X’s shop, X will know that it isn’t B’s card from the signatures unless B has forged the signature. Legally the implications differ in the two cases; in the former case, B is charged with theft only while in the second case, B can be charged with theft and forgery which will ensure that he gets a longer punishment. See: Rupa Mehta and Rohinton Mehta, 2009, p. 4.

but the most predominant form that it takes is that of the ‘Credit Cards’. Plastic money and other forms of electronic payment are nothing but newer and more convenient options of payment. Before entering into the explanation of nature and forms of e-Banking frauds, it is very important to understand e-Banking and modes of payment in e-Banking.

6.3 Nature of the Concept of e-Banking

There are not many inventions that have changed the business of banking as rapidly as the e-Banking revolution. World over banks are reorienting their business strategies toward new opportunities offered by e-Banking. Due to absolute transparency of the market, clients (both the business as well as consumers) can compare the services offered by various banks very conveniently. The seeds of this revolution lie in the ground provided by Information and Commutation Technology (ICT). Progress in Information Technology has slashed the cost of processing information, while the Internet has facilitated its transmission, thus, facilitating change in the very essence of banking business. All around the world, electronic banking services whether delivered online or through other mechanism have spread quickly in recent years. The impact of e-Banking is not limited to advanced economies but also in countries with underdeveloped banking systems.

e-Banking implies provisions of banking services through electronic delivery channels. In India electronic banking has been around for quite some time in the form of automatic teller machines (ATMs) and telephone transactions. In 21st century, it has been transformed by the Internet that is a new delivery channel that has facilitated banking transactions for both customers and banks. For customers, the Internet offers faster access, is more convenient and available around the clock irrespective of the

---

customer's location. For banks, it is a much more efficient and cost saving channel.\textsuperscript{28} As of today, most banks have combined the new electronic delivery channels with traditional brick and mortar branches, but few banks have offered their products and services only through electronic distribution channels. These ‘virtual’ or ‘Internet only’ banks do not have a branch network but also have a physical presence, for example, an administrative office or non-branch facilities like ATMs.\textsuperscript{29} For many customers, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of pay cheque into checking or saving accounts. However, electronic banking involves different types of transactions which are discussed as follows:\textsuperscript{30}

### 6.3.1 Electronic Fund Transfer (EFT)

Few years ago electronic banking was popularly known as Electronic Fund Transfer (EFT). It uses computer and electronic technology as a substitute for cheque and other paper transactions. Electronic Funds Transfer (EFT) is a process by which money is transferred from one bank account directly to another without any paper money. It does not involve the physical presence or appearance of an individual account holder or any kind of physical paper work but uses computers and the Internet for this purpose. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. EFT is safe, secure, efficient and less expensive than paper cheque payments and collections.\textsuperscript{31} It is a process by which money is transferred electronically from one financial institution to another. Merchants and customers tie up with company providing EFT service. EFT company provides specific software to merchant and customers who sign agreement with bank and agree for automatic deduction of money from their bank account. Customer pays online to merchant and sends encrypted

\begin{itemize}
\item \textsuperscript{28} Rupa Rege Nitsure, 2003, p. 5377.
\item \textsuperscript{29} id. Also See: Errol D’Sauza, “How well have public sector banks done?: A Note”, \textit{Economic and Political Weekly}, Vol. XXXVII, No. 9, 2002, pp. 867-870.
\item \textsuperscript{31} One of the most widely-used EFT programs is Direct Deposit, in which payroll is deposited straight into an employee’s bank account. EFT also refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire and point-of-sale (POS) transactions. Retrieved from <http://searchwinint.techtarget.com/definition/Electronic-Funds-Transfer> visited on 2 December, 2012.
\end{itemize}
information using EFT software. Company providing EFT service further sends information to Clearing House Network System. Clearing House Network System approves the customer’s bank account for verification electronically. Bank verifies the transaction and checks for the availability of funds and approves if funds are available and disapproves if funds are not available.\textsuperscript{32}

\subsection*{6.3.2 Direct Deposits}
Direct deposits means electronic funds that are deposited directly into bank account rather than through a paper cheque. Common uses of a direct deposit include income tax refunds and pay cheque. Direct deposit is the most popular form of payment as it eliminates the risk of losing a cheque and eliminates the need to physically visit a bank to make a deposit.\textsuperscript{33} A direct deposit lets consumer authorize specific deposits like pay cheque, social security cheques and other benefits to their accounts on a regular basis. Consumers may pre-authorize direct withdrawals so that recurring bills (like insurance premium, mortgage, utility bills and various club memberships) are paid automatically.\textsuperscript{34}

\subsection*{6.3.3 Phone-By-Phone Systems}
Phone-by-Phone System lets consumers to call their financial institution with instructions to pay certain bills or to transfer funds between accounts. Consumer must have an agreement with the institution to make such transfers. Phone Banking is an additional way to transact business with using regular telephone. It’s a 24X7 banking service which facilitates automated customer interface for account-related inquiries, requests and transactions for call-routing to customer care agents for various product inquiries and other services. It offers convenience at no additional cost. Customers need not to spend time and money for going to the bank and it facilitates to avoid long queues in the branch. This facility also provides information on new product offerings of the Bank on deposits, credit cards, loans, insurance, electronic banking services and

\footnotesize{\textsuperscript{33} Retrieved from <http://www.investopedia.com/terms/d/directdeposit.asp#axzz2Drnxclbj> visited on 2 December, 2012.}
\footnotesize{\textsuperscript{34} Retrieved from < http://www.finance.umich.edu/finops/payroll/forms/directdeposit> visited on 2 December, 2012.}
other products. However, current phone authentication techniques lack security, as they are typically conducted semi-manually, and are susceptible to social engineering attacks like tampering voice. RSA Security has introduced a product that adds voice as a way for automated telephone banking services to identify users. The addition of voice biometrics to its Adaptive Authentication package marks an industry first. The product combines Vocent technology with a voiceprint engine from speech recognition specialist Nuance Communications. This technology product is designed to fight telephone banking frauds.

6.3.4 Personal Computer Banking
Personal Computer Banking is another form of electronic banking. Personal Computer Banking enables consumers to handle many banking transactions via their personal computers. For instance, consumers may use their computers to view their account balance, request transfers between accounts and pay bills electronically. A personal computer banking system is a system in which a personal computer is connected by a network service provider directly to a host computer system of a bank so that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfillment and those requests which are required to be handled by customer service representatives.

6.3.5 Debit Card Purchase or Payment Transactions
Debit Card Purchase or Payment Transactions enables consumers to make purchases or payments with a debit card, which also may be ATM card. This could occur at a store or business online or by phone. The process is similar to using a credit card, with some important exceptions. While the process is fast and easy money transfer is fairly quickly from bank account to the company’s account. So it is important that consumers have funds in their account to cover their purchases. This means consumers need to keep

36 Christopher Young, an RSA vice president, said in the statement: “As we are strengthening security for the web channel, phone banking is effectively becoming the next big target. The product is designed to help to fight telephone banking fraud. This device will recognize the voice of account holder.” Retrieved from <http://news.cnet.com/Telephone-banking-system-recognizes-your-voice/2100-1029_3-6129174.html> visited on 2 December, 2102.
accurate records of the dates and amounts of their debit card purchases, payments, and ATM withdrawals.\textsuperscript{38}

\textbf{6.3.6 Electronic Cheque Conversion}

Electronic Cheque Conversion converts a paper cheque into an electronic payment in a store or when a company receives customer’s cheque in the mail. When customers give their cheque to a cashier in a store, the check is run through an electronic system that captures the amount of the cheque. Consumer is asked to sign a receipt and then get a copy for their records. When customer’s cheque is handed back, it is marked by merchant so that it cannot be used again. The merchant electronically sends information from the cheque to customer’s bank or other financial institution, and the funds are transferred into the merchant’s account.\textsuperscript{39}

\textbf{6.4 Need of e-Banking in e-Commerce}

Need of e-Banking is inherent in the very nature of process of online purchasing in e-Commerce. The basic element of Internet e-Commerce is an e-shop and a server, a user with a web browser and an Internet connection between the two.\textsuperscript{40} The need of e-Banking can be well understood with the detail knowledge of entire process of e-marketing. In e-marketing, the basic element of an e-shop is a web page that offers or advertises the goods for sale and provides a means for the shopper to make the purchase. e-Shops have many more features, these can include: (1) Customer Registration\textsuperscript{41}, (2) Dynamic Web Page\textsuperscript{42}, (3) Personalized Web Pages\textsuperscript{43}, (4) A Shopping


\textsuperscript{41} Customer Registration: Some e-shops first ask the customer to register and then store the customer details on database. This allows the vendor to tailor its information for the specific customer and saves the customer typing in details again on future visits. See: David Whiteley, 2001, p. 191.

\textsuperscript{42} Dynamic Web Pages- The basic web page is formatted in HTML and is then fixed; to change it requires that the source is edited. A dynamic web page is built for each user when it is required by the web browser. The dynamic web page is built by reading a database in which the page include the latest price and possibly whether the goods are in stock. See: David Whiteley, 2001, p. 191.

\textsuperscript{43} Personalized Web Pages- This is another use of the dynamic web page. If the customer is registered with the site, the system can generate a page for that specific customer. See: David Whiteley, 2001, p. 191.
Basket, (5) Additional Information, (6) Multiple Payment options, (7) Encryption, (8) Online delivery, (9) Loyalty Schemes, (10) Online Help and (11) Shopping Mall. Having an e-shop is not of much use if customers are ‘coming in through the door’. A small retailer, with a low investment in their web-site might be content with the level of business that is obtained by chance hits and return visits. However, a large retailer, that has invested a lot in a website, needs to do rather more. Therefore, their ways of advertisement of a web presence and getting customers in through the door includes: (1) Site name, (2) Conventional Advertising, (3) Portals, (4) e-Malls, (5) Search Engines, (6) Links and (7) Personal Shopping Basket: Customers in a conventional shop are likely to collect a number of products in a shopping basket or shopping cart, before coming to the bill and making the purchase. The shopping basket analogy is used in many larger e-shops. Goods can be selected and placed in the electronic basket. Facilities are made available for the contents of the basket to be reviewed and unwanted goods can be returned to the ‘shelves.’ When the shopping is complete, the customer can make payment for the goods in the basket. See: David Whiteley, 2001, p. 191.

Additional information: The e-shop needs to let the customer know what the product or service is. The Internet has both advantages and disadvantages in this area. The customer cannot select some items like perfumes, jumper and chocolates but they can have additional information which is not normally available in a conventional shop. See: David Whiteley, 2001, p. 191.

Multiple Payment Options: The present norm for online payment is a credit card and most e-shops accept all major credit cards. Other modes of payment are debit cards, e-cash (money represented electronically on the web and available for spending with sites that are participants in the schemes) and Payment by phoning the credit card number or posting a cheque. See: David Whiteley, 2001, p. 191.

Encryption: e-Shops are very sensitive to the notion that e-Commerce is insecure, particularly when it comes to secure transmission of personal and payment details. There are various security/encryption schemes in use or being developed. See: David Whiteley, 2001, p. 191.

Online Delivery: Electronic products such as software, information and music can be delivered online. It cuts the cost as well as saves time. Delivery of goods or other products is made through other channel of transportation. David Whiteley, 2001, p. 192.

Loyalty Schemes: Some e-shops are introducing loyalty schemes. Each purchase attracts a number of points and the points, accumulated electronically by the vendor, can eventually be used for discount on goods to a customer. See: David Whiteley, 2001, p. 192.

Online Help: The web page can be used for product instructions and self diagnosis pages—all of which can be updated when the need arises. The customers can also use e-mail for online help.

Shopping Mall: e-Shops may be setup as a part of an online mall. Like conventional equivalent the online mall is designated to attract customers because there is a range of stores. E-malls can help out the individual vendors with shared facilities, for instance a common customer file and a shared payment infrastructure. See: David Whiteley, 2001, p. 192.


Site Name: The surest way of finding an e-Commerce site is the URL. A simple site name can be guessed by users and might be easily remembered. See: David Whiteley 2001, p. 193.

Conventional Advertising- An irony of e-Commerce is the apparent urge to advertise them through conventional media in a newspaper, television and on the carrier bags in real shops. Conventional advertising of Internet addresses has a three fold effect- (1) It boosts the image of the organization and any conventional facilities it might have-it gives an air of modernity and ‘high-tech’ facilities. (2) It lets the customer know that the organization has Internet facilities. (3) It can give users access via the url. See: David Whiteley, 2001, p. 193.

Portals: On loading the browser and connecting to the web, users are met with a first page. This page is portal, the place from which to access the facilities of the Internet. The portal is a valuable piece of property. It is the one place through which all users are likely to pass. Advertisements on the portal can be banners. Portals provide a menu of services and inclusion in that list is another way of picking up business. See: David Whiteley, 2001, p. 193.

Malls: The Internet shopping mall means a lot of shops under one roof with a pleasant shopping atmosphere. To own a shop in a conventional mall is usually a good way of getting noticed by
Recommendations. It depends on the skills of vendor in e-Commerce marketing. Once a consumer satisfies and decides to purchase a commodity, then the next important step is to place online orders. On a website a very common icon is shopping basket or shopping cart. In e-shop that is selling tangible goods, the customer is invited to browse round the shop, select goods and put them in his/her basket. On a good site the contents of the basket can be inspected at any time, the total value of the goods is shown and any of them can be ‘returned to the shelves’ if the customer decides against the purchase. Service sites indicate their own process of purchase. The checkout involves filling in a form. The form filing is optional for customers who are pre-registered and have not subsequently lost their passwords. For the payment the customer has to provide a credit card number and for delivery his/her name and address. Payment of goods and services bought using the web is made through e-Banking. For a retail transaction, the norm is that the payment is made at the time of purchase coincident with the exchange of goods. The retailer takes cash, cheque or a credit/debit card as payment and the customer takes the goods. To replicate retail trade exchanges online, there is need for a way of transferring value electronically. The ways of payment in e-Commerce transaction are: Credit Cards, Debit Cards, Store Value Cards, e-Cash, Smart cards and online payments. Here lies the need or origin of e-Banking in e-Commerce. Any contract without payment of money (consideration) will not be valid, therefore, the payment of money in online shopping is entirely based on e-Banking. The marketplace has very tactfully responded to concerns of consumers. A few basic models or approaches to net-based sales transactions have come into focus. They are:

---

57 Customers. The intention of an Internet mall is same, hopefully the customers who have been there before come back again. See: David Whiteley, 2001, p. 194.
58 Search Engine is a standard way to find any Internet site and that includes e-shops. A successful e-shop can appear in the top ten lists of search engine the customer uses. A site owner, who knows the tricks of the trade, can submit information to a search engine that ensures they get listed. The search engines list only a small number of the sites that are there on the Internet. See: David Whiteley, 2001, p. 196.
59 Links: Online advertisements on the web also link to the site-hypertext links. Links include a variety of other sites with a variety of deals being done. See: David Whiteley, 2001, p. 196.
59 The final way of getting customers onto the site is the personal recommendation. The satisfied customer will bookmark the site, comeback to the site again and recommend it to their other friends. See: David Whiteley, 2001, p. 196.
60 ibid., pp. 200.
61 ibid., pp. 200-201.
Model I: The consumer, responding to net-based marketing presentation, sends in a cheque, or calls and verbally transmits a credit card, over the merchants telephone. This is fairly a traditional approach, and no financial transaction takes place on the Internet.

Model II: The consumer (i) sets up account with a merchant or a third party organization; (ii) leaves his or her credit card number by means other than Internet; and (iii) gives the merchant the authorization to bill the account, whenever the consumer chooses to buy something.

Model III: The consumer leaves his or her credit card number on an unsecure online order form. With this approach, the consumer is put at some risk and the credit card number can be compromised, but the risk is perhaps not much greater than giving it out over the phone.

Model IV: The consumer uses a secure (encryption) client software program to transfer his or her encrypted credit card number to secure (decrypting) merchant server.

Model V: The consumer exchanges traditional currency (cash, cheque, credit card authorization) for some form of digital currency, and then spends units of that currency whenever and wherever he or she likes. This requires some form of “electronic Wallet” to hold the currency and an account set up between the currency provider and the participating merchants.

It is observed by the researcher that out of all the modes of payment, the most risky mode is when consumer leaves his or her credit card number on an unsecure online order form. This research is focused on risks to customers’ account number during e-Banking at the time of online shopping. For a microscopic study of nature of e-Banking frauds, a close look is given to various modes of payment electronically.

6.5 Payment Mechanism in e-Commerce: A Microscopic Reflection

The idea of paying for goods and services electronically is not a new one. Since the late 1970s and early 1980s, a variety of schemes have been proposed to allow payment to be
effected across a computer network. The arrival of the Internet has removed all the obstacles on the path to progress. This network of networks has grown dramatically from its inception in the late 1970s to today’s global medium. The initial focus of electronic commerce was on selling goods to consumers (B2C). Around 1999, the industry focus began to shift to the trade that businessmen and companies do with each other (B2B). In both the B2C and B2B sector, the web was first used simply as a means of discovering products and services, with the payment being carried out offline. Now a days, in an online electronic marketplace, a huge variety of different payment methods has been developed.\textsuperscript{63}

Electronic payment refers to paperless monetary transactions or e-payment. Payment through electronic modes has benefited e-Commerce businesses and has supported financial institutions. Electronic payment is exchange of finances that takes place online between buyers and sellers. The content of this exchange is usually in the form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary or by a legal tender.\textsuperscript{64} A wide range of systems have been developed for online payments. It is divided into account-based and electronic currency systems. Account-based systems allow payment via an existing personalized account (usually a bank account), whereas electronic currency systems allow payment simply if the payer has an appropriate amount of electronic currency. Five different forms of account-based systems are described: i) Credit cards, ii) Debit cards, iii) Mediating systems, iv) Mobile payment and Telephony account systems, and v) Payments via online banking. Electronic currency systems can be divided into (i) e-Money or e-Cash and (ii) e-Wallets or Digital Wallets.\textsuperscript{65} There are various types of generic payment systems which are discussed as under-


6.5.1 Credit Cards

A credit card is one of the primary tools of an e-payment system in e-Commerce. It is explained as a payment card, the holder of which is permitted under his/her contract with the issuer of the card, to discharge less than the whole of any outstanding balance of his payment on or before the expiry of a specified period (subject to any contractual requirements with respect to minimum or fixed amount of payments). The credit card issuer sends the card holder periodic statements (usually monthly) describing the purchases made. The card holder may settle the indebtedness without interest by paying the entire amount on receipt of the statement or the card holder may settle the indebtedness by installments, paying interest on the outstanding amount.66 Thus, the credit card embodies two essential aspects of the basic baking function (i) the transmission of payments; and (ii) the granting of credit.67 When a consumer owns a Credit card, the credit card bank supports consumer financially to buy products at the time of purchasing. If a consumer has a credit card of XYZ bank, it is not necessary to have sufficient account in that bank. When consumer purchases something and pay by a credit card, he/she can pay the bank back after a certain time period depending on the number of days specified by the bank, along with the payment for the other purchases he/she made that month.68 This flowchart depicts the workflow of a credit card used for electronic payment. When the credit card issuing bank approves the payment transaction, the information passes in the reverse mode and finally credit card holder receives the transaction confirmation. It is shown as under:69

---

66 A credit card is a small plastic card with a unique number, which identifies the account. The credit card has an expiration date and its own identification number. Most credit cards also have a magnetic strip embedded in it for automatic entry via a card reader. Credit cards are not only used for day-to-day financial transactions but have become very popular in e-Commerce transaction payment. Credit card is a card whose production enables the person to whom it is issued (the holder) to discharge his obligation to a supplier in respect of payments for acquisition of goods, services, accommodation or facilities e.g. VISA, Master Card, American Express and the like. See: Sarla Gupta and Beniprasad Agrawal, Information Technology Law and Practice, Premier Publishing Co., Allahabad, 2009, p. 286.
69 id.
User submits personal information on e-Commerce Web-site

User Information in encrypted form is transferred to the merchant server

A payment gateway receives encrypted information from merchant server and transfers to merchant processor

Merchant processor sends authorization request to the credit card issuing company

Credit Card issuing company passes the request to the credit card issuing bank

Approved

Rejected

Authenticated information sent back to the e-Commerce website

Transaction cancelled

Transaction processed

Diagram-Workflow for a Credit Card

6.5.2 Debit Cards

A debit card is a small plastic card with a unique number which identifies the account. The debit card also has an expiration date and its own identification number. Most debit cards also have a magnetic strip embedded in it for automatic entry via a card reader. If consumer has the debit card of a bank, it is necessary to have sufficient account (amount) in that bank. It other words, when consumer makes payment using a debit card, the money is deducted immediately from his/her account unlike with the credit cards where consumer gets time period to repay the amount to the bank that issued the credit card. There are two types of debit cards.  

---


6.5.2.1 Online Debit Cards

In online debit cards, such as an ATM, the money is transferred from customer’s account to the merchant’s account immediately. The PIN is required to access the debit card. The online debit cards are connected to regional banking systems of country. With online debit cards, customer must enter a Personal Identification Number (PIN) and authorization and settlements occur immediately.

6.5.2.2 Offline Debit Cards

In offline debit cards, the merchant’s debit card reading device stores customer’s debits and instead of using the PIN, customer can physically sign the receipt given by the merchant to customer. In offline debit cards, the processing takes approximately two to three days. With the VISA and Master Card offline debit cards, electronic authorization is immediate, but settlement can take a few days.\(^72\)

6.5.3 Smart Cards

Smart cards were invented by the Frenchman Roland Moreno, who patented the idea in 1974.\(^73\) Smart Cards incorporate a microchip, which stores information about the cardholder and his bank account. Smart cards facilitate the electronic funds transfer at the point of sale (EFTPOS). After the computer has checked that the customer has sufficient funds or credit facilities, the sum is transferred straight into the beneficiary’s bank account, thus eliminating both the need for any cash or paper transaction and the retail merchant’s problem of ‘bounced cheques.’\(^74\) Smart cards can also hold details at a

---

\(^72\) Debit cards look very much like credit cards but function differently as they do not offer ‘credit’ to the user of the card. The debit card is linked directly to the user’s bank account. Whenever any purchase is made using the debit card, the amount gets deducted from the saving account and is transferred to the beneficiary’s account. Thus, if the card-holder does not have a balance in his account, he/she cannot use his/her card. Such cards are very conveniently used by people. Such cards are generally in the form of store cards, petrol cards etc. In developed countries, store chains such as Sears, K-Mart issue such cards to their customers for their convenience and for expediting check-out of items and payments. See: Rupa Mehta and Rohinton Mehta, 2009, p. 15. Retrieved from <http://www.english.rfi.fr/france/20120430-french-smart-card-inventor-moreno-dies-paris> visited on 21 August 2012. The Frenchman who invented the internationally recognised Smart card has died in Paris aged-66. Roland Moreno has become an essential part of phone cards, bank cards and SIM cards worldwide. Today, the French company, Gemplus, is the world’s leading smart card manufacturer and the French are the world’s leading smart card users.

\(^73\) Retrieved from <http://www.english.rfi.fr/france/20120430-french-smart-card-inventor-moreno-dies-paris> visited on 21 August 2012. The Frenchman who invented the internationally recognised Smart card has died in Paris aged-66. Roland Moreno has become an essential part of phone cards, bank cards and SIM cards worldwide. Today, the French company, Gemplus, is the world’s leading smart card manufacturer and the French are the world’s leading smart card users.

time up to 200 past transaction undertaken using the card. Smart cards keep track of the money spent by the user and prevent duplicate transactions. A special device called a smart card reader is required for accessing a smart card. Smart cards can be accessed only with the unique PIN of an individual. Smart cards are secure because they are in encrypted form and a user can personally encrypt or decrypt the data stored in the chip of a card.\textsuperscript{75}

6.5.4 \textit{Automated Teller Machine (ATM) Cards}

An automated teller machine or automatic teller machine (ATMs) are known by various other names including ATM machine (America and Australia), Automated Banking Machine (ABM in Canada), “Cash Dispenser” (Germany) and “Cash Point”, “Cash Line” or “Cash Machine” (British English).\textsuperscript{76} The early 1980s saw the growth of multi-functional Automated Teller Machines. The ATMs are computer linked and provide a wide range of banking services. These are operated by plastic cards carrying a magnetic strip recording the card holder’s personal details. The ATM card-holder is given a personal password which after he/she has inserted the card in the machine, he/she enters into the keyboard. This action links the machine with the bank’s computer. The ATM facility allows the customer to do enormous functions like:\textsuperscript{77} (i) Withdraw cash; (ii) Know the balance in account; (iii) Enable customer to order for a cheque book; (iv) Enable customer to carry out a transfer of amount from his account to another account of the same bank; (v) To deposit in his account cash or cheques, at times even without completing a paying-in slip; (vi) To settle telephone and utility bills; (vii) Quicker transactions; (viii) Reduction in labour work, paper work and documentation and (ix) Increase in the number of customers who can be served. The ATMs facility is the most visible face of electronic banking.

\textsuperscript{75} A smart card looks similar to credit and debit cards. It has a plastic body and a microprocessor chip embedded in it. With the growth of e-Commerce transactions, smart cards definitely have played a major role in the success of electronic payment. As compared to credit and debit cards, smart cards are less expensive and provide faster transaction processing. Making a payment with a smart card saves a lot of time because the smart card and chip contains details about the owner in a non-encrypted form and the user does not have to explicitly provide details for verification. See: NIIT, 2004, p. 19.


\textsuperscript{77} Rupa Mehta and Rohinton Mehta, 2009, p. 11.
6.5.5  e-Money

In e-Money transactions, the payment is sent across the network and the amount is transferred from one financial body to another without a middleman. This mode of payment is faster, more convenient, and saves a lot of time, energy and money. e-Money is available in two forms today- (a) Card form wherein cards can be acquired physically such as Credit Cards, Debit Cards and Smart Cards; (b) Computer Software form which is available in the form of software such as e-Wallets and e-cash. Most of the prominent forms of e-money are: e-cash and e-Wallet

6.5.5.1  e-Cash

The concept of e-Cash has been developed by Dr. David Chaum. It is widely used for small payments on the Internet. When a customer pays online via e-Cash, the amount is directly transferred from customer’s bank account without any medium in between. In order to use e-Cash, the user and the merchant both have to sign up with the bank or company issuing e-Cash. Digital cash or e-cash is one of the first forms of alternative payment systems developed for e-Commerce. e-Cash involves four major components- (1) e-Cash issuing company (This could be either a bank or another non-banking institution); (2) e-Cash users (Users are the people who use e-Cash for electronic payments); (3) Merchants (They receive the e-Cash payment); and (4)

---

79 Retrieved from <http://cryptome.org/jya/digicrash.htm> visited on 13 December, 2012. This name of Dr. David Chaum one man stands out way above anyone else in the history of Digital Cash: David Chaum, US citizen, born into a wealthy family, brilliant mathematician. After travelling around the world he ended up in Amsterdam in the late 80’s. He became head of the cryptography department of the CWI (Centre of Mathematics and Information Science). Cryptography is the science of encoding and decoding of data, in order to maintain privacy. Dr. David Chaum had built a big reputation in this field in the previous few years.
80 The basic idea behind all digital cash systems is payment over the Internet by transmitting unique, authenticated tokens representing cash value from consumer to merchants. In these schemes, users would deposit money in a bank. Banks would issue digital tokens (unique encrypted numbers) for various denominations of cash, and consumer could “spend” these at merchant’s sites. Merchant would in turn deposit these electronic tokens in its bank. Some firms such as e-Gold and Goldmoney have focused on electronic currency backed by gold bullion. e-Gold is probably the best known of these firms. Originally established in 1996, E-Gold Ltd., a company organized under the laws of the country, offers an electronic currency. It is called e-Gold. See: Kenneth C. Laudon and Carol Guercio Traver, e-Commerce: Business, Technology and Society, Pearson Education, Delhi, 2008, p. 310.
Regulators (They are the government bodies that regulate the flow of e-Cash). This diagram shows the workflow of e-Cash.\(^81\)

---

**Diagram: Workflow of e-Cash**

The workflow of e-Cash depicts that the chances of the theft of e-Cash are nil because the owner does not physically own it. However, there is a possibility of a hardware or software failure in a PC on which the e-Cash is stored. The most important advantage of e-Cash is that it can be used for online transaction between a customer and a website or between two individuals.\(^82\)

### 6.5.5.2 e-Wallet or Digital Wallet

e-Wallet can be used through the e-Wallet software, which can be downloaded from the website (www.eWallet.com). An e-Wallet is stored on the user’s personal computer. Once the e-Wallet software is downloaded from a website, it is ready to use. The user needs to fill in the details, followed by encrypting it on the hard disk of a PC with unique PIN. The information can be updated offline because the e-Wallet is stored on the user’s PC.\(^83\) An e-Wallet is purely in an electronic form unlike a credit or debit card that is physically owned by the owner. An e-Wallet is used for very small payments. Most web-sites provide their own site-based e-Wallet payment option to customers,

\(^81\) NIIT, 2004, p. 21.
\(^82\) id.
which can be used by just clicking on the site-based wallet. An e-Wallet follows a stored value system in which some amount is deposited in advance in the Wallet. For every electronic payment made through e-Wallet, the amount is reduced automatically from the account.\textsuperscript{84} A digital wallet seeks to emulate the functionality of a regular wallet that he/she carries. The most important functions of a digital wallet are: (a) to authenticate the consumer through the use of digital certificates or other encryption method, (b) to store and transfer value and (c) to secure the payment process from the consumer to the merchant.\textsuperscript{85}

6.5.6 \textit{Pay Pal (Person to Person) Payment}

Pay Pal\textsuperscript{86} is a very sophisticated payment mode in which he/she can send money through e-mail. A PayPal account is associated with a user’s regular bank account. Once a transaction takes place, PayPal sends an e-mail to both the sender (who used PayPal to send the money) and the receiver (who received the money through PayPal). A PayPal (person-to-person) online payment is sometimes also referred to as P2P. PayPal can be used for electronic payment through PC or a web-enabled mobile phone. Online payment can be made not only to a merchant’s web-site but also to other consumers through e-mail. Through PayPal, a person who is not a member of PayPal can also receive payment via e-mail but in order to access it, they would need to sign up with the PayPal Company. This diagram depicts the working of PayPal in a flow chart:\textsuperscript{87}

\textsuperscript{84} NIIT, 2004, p. 22.
\textsuperscript{85} Lincoln D. Stein, \textit{Web Security: A Step-by-Step Reference Guide}, Reading, Addison-Wesley, MA, 1998, p.101. Early efforts by many companies failed to popularize the idea of digital Wallet. Even Microsoft, which offered a proprietary server-side digital wallet with first passport and then MSN wallet, ultimately abandoned the effort in February 2005. The latest effort to develop something like a digital wallet is Google’s Checkout, which is a payment processing system designed to make online shopping more convenient and easier. It does not store value like PayPal, but communicates a shopper’s credit card and personal information necessary for a transaction to the merchant. The merchant receives some additional transaction guarantees that the user has been authenticated by Google. It is not clear at this time how successful this system will be. See: Kenneth C. Laudon and Carol Guercio Traver, 2008, p. 300.
\textsuperscript{86} Pay Pal was launched in November 1999. A PayPal account is associated with a user’s regular bank account or credit card. PayPal is a global e-Commerce business allowing payments and money transfers to be made through the Internet. Online money transfers serve as electronic alternatives to paying with traditional paper methods, such as cheque and money orders. Retrieved from <https://www.paypal-apac.com/sg/about-paypal/history-of-paypal.aspx> visited on 15 December, 2012.
\textsuperscript{87} NIIT, 2004, pp. 24-25.
6.5.7 **Digital Accumulating Balance Payment System**

Digital Accumulating Balance Payment System allows users to make micropayments and purchases on the web, accumulating a debit balance for which they are billed at the end of the month. Like a utility or phone bill, consumers are expected to pay the entire balance at the end of the month using a checking or credit card account. Digital accumulating balance systems are ideal for purchasing intellectual property on the web such as single music tracks, chapters of books, or articles from a newspaper, ringtones and games. Balances accumulate and customers are billed monthly with their regular phone bill.\(^{88}\) A good example is Valista’s Payments Plus, a system for accumulating balances for small transactions. PaymentsPlus is used by companies such as Kiosk, emitra, AOL, Vodafone, DoCoMo, Tiscali, Wanadoo and T-Online. Mondex\(^ {89}\) technology also assists consumers in online shopping in a safe and secure environment.

6.5.8 **Auripay**

The technology involves use of an Auripay number which is formatted like a credit card number and which can be deactivated after a single use. These numbers may even be

---

\(^{88}\) Kenneth C. Laudon and Carol Guercio Traver, 2008, pp. 311-312.

\(^{89}\) Mondex was conceived offline and is migrating towards the Internet. Mondex is entirely chip card- based, and it is unique in the sense that it can accommodate card-to-card transfer. Mondex uses bearer certificates; funds are stored remotely on the user’s actual card. Unlike e- Cash, Mondex funds can be transferred from one card to another indefinitely without requiring central clearing or verification by a bank or processor. However, this e-payment method has become obsolete. See: Karnika Seth, *Cyber Laws in the Information Technology Age*, LexisNexis Butterworths Wadhwa, Nagpur, 2009, p. 289.
customized based on some parameters like: number of times a number can be used, amount limit of a particular transaction, card holder’s name and address, stored value card, merchant specific card and time limit on the Auripay or expiry date. In case unauthorized person gains access to these numbers, he/she will not be able to use it because Auripay will deny authorization. The consumers may obtain Auripay numbers simply by clicking on their web browser while they are shopping online.90 The Auripay numbers can be used at any site that accepts credit cards. This system is designed to work in parallel with the bank transaction system without interfering with their day to day transactions. At the time of issuing an Auripay number the appropriate amount of money will be transferred from the consumer bank account to the Auripay account in the same bank. This eliminates the credit liability from both the Auripay account and the bank. During settlement at the end of the day money is transferred from local account to Auripay account with the VISA or Mastercard networks. Once the money is transferred the network will settle with the merchant. This system has many advantages, particularly in that it does not require specific hardware for either the user or e-merchant. Credit card information is not disclosed to the merchant. Moreover, it is possible to use this site at any site allowing payment by credit card and merchant do not have to register with Auripay.91

6.5.9 Mobile Banking (M-Banking)

A new revolution in the realm of e-Banking is the emergence of ‘Mobile banking’. Online banking is now moving to the mobile world, giving everybody with a mobile phone access to real-time banking services, regardless of their location. According to this novice system, customer can access account details on mobile using the Short Messaging System (SMS) technology where select data is pushed to the mobile device. The wireless application protocol (WAP) technology allows user to surf the Internet on their mobiles to access anything and everything. Mobile e-Pay allows mobile network operators or mobile Internet Service Providers (ISPs) to act as a portal content or service providers to handle financial transactions using mobile phones.92 Reserve Bank of India had set up the Mobile Payments Forum of India (MPFI), a ‘Working Group on

Mobile Banking’ to examine different aspects of Mobile Banking (M-banking). The Group had focused on three major areas of M-banking, i.e., (i) technology and security issues, (ii) business issues and (iii) regulatory and supervisory issues. This new innovation, its consequences and its legal impressions are out of orbit of this research.

6.6 Frauds in Online Payment Mechanism of e-Commerce

“There are three things in the world that deserve no mercy; hypocrisy, fraud, and tyranny.

Frederick W. Robertson

It is beautifully said that ‘Fraud’ is the ready minister of injustice. In simple words, fraud can be defined as willful deceit or trickery or a deception or spurious thing. Since times immemorial fraudulent activities are deeply embedded in business. In Indian physical banking industry, the classification of banking frauds are used to be like: Misappropriation, Criminal breach of trust, Fraudulent encashment through forged instruments, Manipulation of books of account or through fictitious accounts, Conversion of property, Unauthorized credit facilities extended for reward or for illegal gratification, Negligence, Cash shortages, Cheating, Forgery and Irregularities in foreign exchange transactions. Till today frauds are committed on consumers in banking sector, however, modes of frauds have become very refined and sophisticated. On one hand, technological advancements have provided a bundle of facilities to consumers in Cyber world, however, on the other hand, novice modes of committing frauds have also come into existence which are very difficult to recognize and investigate. Frauds like brand spoofing, phishing, pharming, identify theft and other online frauds continue to be a major issue of retail banking and banks all over the world. The focus of this research is on the frauds committed with innocent consumers in an online Banking or Internet banking during online shopping. The frauds in e-transactions have been discussed in following headings:

---

6.6.1 Cyber Money Laundering or e-Money Laundering

Cyber Money Laundering is a complicated and multistage process that can consist of many single transactions.\textsuperscript{95} Cyber Money Laundering is a common variety of financial crime. It means a fraudulent way of accessing the credit card numbers of several persons when their monetary transactions are taking place and then transferring the currency to one’s own account or using it for one’s own benefit. In general parlance, the word “laundering” refers to ‘wash and iron the clothes’ but in the context of cyber financial frauds, it has acquired a new meaning and it denotes ‘a process by which cash derived from a criminal enterprise may be easily exchanged without a trace of its origin.’\textsuperscript{96} The term ‘money laundering’ was used in legal context for the first time in the Watergate Scandal case of United States in 1973 and it meant, “a progress of converting money derived from illegal activities into a legally consumable form.” Therefore, in other words, money laundering is a cybercrime in which money is illegally downloaded while it is in transit.\textsuperscript{97} Hawala is a special kind of underground banking system, which is considered highly efficient means to launder money.

e-Money laundering is not a single act but it is derivative crime which involves three basic steps, namely, (i) Placement (ii) Layering and (iii) Integration. It means “placement” of the dirty money into the financial system; “layering”, where the dirty money, that is present in the banking or financial system, is moved through the global financial system to hide its origin or separate it from its illegal source, and “integration”, where the illicit funds are blended back into the economy and become indistinguishable from legitimate funds.\textsuperscript{98} Money laundering is one of the most common financial activities connected to illicit financial schemes, tax evasion, narcotics, corporate frauds, government corruption and white collar crimes. The beauty of money laundering is that it touches them all and danger of money laundering is that it goes on


\textsuperscript{98} ibid., p. 45.
without being identifiable because the larger picture becomes missing due to incomplete understanding of what money laundering is, how it works, and who is involved.  

### 6.6.2 Credit Card Frauds

Credit Card holds a very important place in today’s life. Credit cards are a popular form of payment for any person in online purchases. People use them every day without thinking very much about their specific risks. Credit cards offer a wide range of advantages to consumers allowing them to shop without carrying cash and to buy expensive items. There are two very famous methods for committing frauds with credit cards. Firstly when a consumer/person/card holder genuinely loses his/ her card or when he/ she forgets to collect it from cashier after payment of goods or when he/ she loses his wallet with his/ her card. Secondly, when card of card-holder is stolen fraudulently. Card can be stolen from wallet, purse, house, car and shop etc. In this case if any person (card-holder) has written password on the back side of the card, he/she is going to face huge financial loss. Other than the cases wherein credit card is not lost or stolen, frauds are committed which are explained as under:

#### 6.6.2.1 Merchant Collusion

Merchant collusion is said to occur when the merchant colludes with the fraudster by providing information regarding genuine credit cards, in return for a share in the fraudulent amount. The merchant can allow members of a gang to use his terminal as a host in order to transfer information on credit cards, which are swiped on his terminal. The fraudster’s terminal, known as the receptor, since it receives the information, downloads the genuine card details from the host terminal. This information can be used in various ways in order to defraud the issuer at a later date, at the convenience of the fraudster. The information can be used to manufacture counterfeit cards or to obtain genuine cards by reporting the card as lost or to defraud by mail order.

---


102 ibid., pp. 146-147.
6.6.2.2 White Plastic Card Fraud

White plastic card fraud is fraud perpetrated by using a blank piece of plastic. The gang of fraudsters uses credit card information, which has been downloaded from host terminals (merchant collusion) or obtained through their contacts in credit bureau or at the issuer’s collusion by embossing on the plain blank pieces of plastic. After comparing with the fraudulent merchants, fraudster can take as many imprints of the various cards he wants for any amount that he feels is right, forges the signature on the charge slip and then present it to the acquirer for payment. The fraudulent earnings are obviously shared by the colluding parties. By the time the banks realize that the charge slips are of fake cards, the payment has already been made to the merchant. In white plastic fraud, it is not difficult to identify that the imprint is that of a fake card because the embossed figures of the card pin number are crooked and follow the same font or pattern as the original card. The reason why it is rarely detected before the payment is made is that the staff is either not trained properly for it or they are overworked, that’s why they do not have the time to scrutinize each chargeslip as closely as it deserves to be.103

6.6.2.3 Skimming

CVV (Customer Verification Value) means a combination of features used in credit, debit and automated teller machine (ATM) cards for the purpose of establishing the owner’s identity and minimizing the risk of fraud. The CVV is also known as the Card Verification Code (CVC) or Card Security Code (CSC).104 Skimming is the fraudster’s answer to the CVV (Customer Verification Value) introduced by the issuers. CVV is an algorithm (a code) which is very difficult to break through. The fraudster, therefore, does not bother to do so. He (fraudster) simply colludes with a merchant or merchants. He/ She then provides the merchant with a terminal similar to the one provided to the merchant by the bank. The difference being that the fraudster’s terminal is capable of actually recording the data on each magstripe which is swiped through the terminal while the banks terminal only processes the data but does not have a recording facility.

103 ibid., p. 148.
The merchant swipes the card twice; once on the bank’s terminal and again on the fraudster’s terminal. The CVV which is encoded on the magstripe, and is decoded on the terminal gets recorded on the fraudster’s terminal. The fraudster has now genuine card information along with the CVV for each card. This is a goldmine for making counterfeit cards as far as the fraudster is concerned.\textsuperscript{105}

\textit{6.6.2.4 Terminal Takeover Fraud}

This is a variation of the ‘Skimming’. In this fraud, the fraudster does not collude with the merchant; instead he presents himself/herself as the employee and proceeds to examine the working of the terminal. He will find a fault in the machine and replace it with another machine. This machine is capable of performing the same functions as that of the bank’s terminal and in addition it also has the facility to store the credit card information obtained through the magstripe. After a few days, the fraudster returns with the acquirer’s machine claiming that it has been repaired. He replaces his own machine with the original machine and disappears along with all the confidential credit card data.\textsuperscript{106} This type of fraud is committed with merchants or people who very ignorant as well as negligent about emerging crimes in society. It is submitted that from the last five years, such frauds have not been reported.

\textit{6.6.3 Phishing}

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email with an intention to gather personal and financial information from recipients. In this type of fraud the messages appear to come from well known and trustworthy web sites. Web sites that are popularly and frequently spoofed by phishers are highly effective against some forms of online frauds. For example, if the data in the magnetic stripe is changed, a stripe reader will indicate a “damaged card” error. The flat-printed CVV is routinely required for telephone or Internet-based purchases because it implies that the person placing the order has physical possession of the card. Some merchants check the flat-printed CVV even when transactions are conducted in person. However, the CVV technology cannot protect against all forms of fraud. If a card is stolen or the legitimate user is tricked into divulging vital account information to a fraudulent merchant, unauthorized charges against the account can result. A common method of stealing credit card data is phishing, in which a criminal sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Once the criminal has possession of the CVV in addition to personal data from a victim, widespread fraud against that victim, including identity theft, can occur.


\textsuperscript{106} Rupa Mehta and Rohinton Mehta, 2009, p. 150.
include PayPal, eBay, MSN, Yahoo, BestBuy and other bank websites. A phishing expedition, like the ‘fishing’ expedition it’s named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishing is an e-mail scam where the fraudster leads the card-holder to believe that he is responding to a legitimate e-mail request from a known or well-known organization. The working of this scam is explained as under:

1. Card-holder receives an e-mail from a well-known organization or bank etc. requesting him/her to update his personal information for ‘security reasons’ or for ‘updating’ their existing’ records.

2. The fraudster ensures that the site looks as the genuine site including the logo, company name, address etc. In fact, they do such a good job that very often, even if the card-holder has been to the original site many times, he/she will not spot the difference.

3. The e-mail will have a link, which the card-holder will be directed to click on for updating the records.

4. When the card-holder clicks on the link, he/she will be asked to fill out a short form giving his personal details such as: (a) Name (b) Address (c) Card Number (d) PIN and (e) CVV.

5. Many card-holders provide this information believing that they are responding to their own bank or some known merchant.

6. Fraudsters gather this data and use it to either transfer funds into their own accounts or to buy goods online which they can sell later. The transfer and purchases are made immediately. By the time the card-holder realizes that he has been duped, the fraudsters have made away with the money and goods. Some fraudsters go a step further when they request the recipient of the mail to download and install ‘security’ software that will protect them. If the software is installed, the fraudster can monitor the computer and capture card and bank account details. Often, the spam e-mail itself is sent from an unsecured computer.

or server that the fraudster has taken over. It is submitted that in our mailbox, every day we receive emails from HDFC Bank, Punjab National Bank, ICICI, State Bank of Patiala, Dena Bank or from any of the bank in which we or our family member have account asking for our personal financial details. If anyone fills these details, these details can be misused.

Phishing is a deceptive online attempt by a third party to obtain confidential information for financial gain. Phishing attacks do not involve malicious code but instead rely on straight forward misrepresentation and fraud, so-called ‘social engineering’ techniques. The most popular phishing attack is the e-mail scam letter. Thousands of phishing attacks use other scams in addition to “Nigerian Letter Scam”, some pretending to be eBay, PayPal or Citibank writing to you (anyone) for “account verification”. Click on a link in the e-mail takes that person (consumer) to a website controlled by the scammer, and asks him/her to enter confidential information about customer’s accounts such as bank account number and PIN Codes. Some people disclose their personal account information. Phishers use this information to commit fraudulent acts such as charging items to customer’s credit cards or withdrawing funds from customer (his/her) bank account, or in other ways “steal his/her identity.” Phishing attacks are one of the fastest growing forms of e-Banking crime.

Phishing on Internet is a form of Passing Off. Phishing is a form of Internet fraud by using passing off tactics where a person pretends to be legitimate association such as a bank or an insurance company in order to extract personal data from a customer such as his access codes, password etc. The personal data so collected by misrepresenting the identity of the legitimate party is generally used for siphoning out money from the victim’s account. The High Court of Delhi in its decision in the case of National

---

110 This scam begins with an e-mail: A rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive a million dollars. This type of e-mail scam is popularly known as a “Nigerian Letter” scam.
Association of Software and Service Companies vs. Ajay Sood and Others,\(^\text{113}\) is considered as a landmark decision in the history of Indian Cyber crimes for two obvious reasons. Firstly, phishing is punishable as cyber offence although there is no specific statutory legislation to this effect; and secondly, it reaffirms the faith of intellectual property owners in their intangible property because now their rights are well protected by the judiciary. The Court in this case expressed a view that of late, phishing has developed as a sophisticated method of committing organized cyber crime by befooling even the most experienced and knowledgeable persons. Phishing criminals sneak into a computer network or a social networking site and obtain e-mail addresses of the people and create messages that purport to come from direct bosses. They manipulate legitimate websites to redirect e-mails to bogus sites that collect victim’s information.

6.6.4 Pharming

Hackers who attempt to hide their true identity often spoof or misrepresent themselves by using fake e-mail addresses or masquerading as someone else. Spoofing a web site is also called “pharming”, which involves redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker. The word “spoof” means to hoax, trick, or deceive. Therefore, in the world of Information Technology world, spoofing refers tricking or

\(^\text{113}\) In this case, the plaintiff i.e. National Association of Software and Service Companies having its trade name NASSCOM, the India’s premier software association and the defendants were running an employment agency providing employment and recruitment opportunities to job-seekers. In order to obtain personal data, which they could use for the purpose of recruitment, the defendants composed and sent e-mails to the concerned parties in the name of NASSCOM. On a complaint from the plaintiff, the High Court of Delhi passed ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to NASSCOM. The Court further restrained the defendants from representing themselves as being associated as a part of NASSCOM and ordered a search of the defendant’s premises by a local Commission. On the basis of two hard disks of computers recovered from the defendants it was found that the e-mails were sent by the defendants to fictitious persons in order to hide their illegal fraudulent activities. The investigation also revealed that the defendants had collected huge amount of money by fraudulently using the NASSCOM’s trade name. Finding no other way to escape liability and punishment, the defendants admitted their crime and the parties agreed to a mutual compromise under which the defendants were to pay 1.6 million rupees to the plaintiff’s by way of damages for violation of plaintiff’s trade name rights. The hard disk seized from the defendant’s possession was ordered to be handed over to the plaintiff who would be the sole owner of those disks. The judgment in the case was delivered by the Delhi Court on March 12, 2005. 119(2005) DLT 596, 2005(30) PTC 437 (Del.).
deceiving computer systems or other computer users. This is typically done by hiding one’s identity or faking the identity of another user on the Internet. Spoofing can take place on the Internet in several different ways, namely, (i) e-mail Spoofing\textsuperscript{114} (ii) IP Spoofing\textsuperscript{115} and (iii) Spoofing can be done by simply faking an identity\textsuperscript{116}. Although spoofing does not directly damage files or network servers, it threatens the integrity of a site. If hackers redirect customers to a fake web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site. Or, if the intent is to disrupt rather than steal, hackers can alter orders, change products ordered and then send them to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment and the company may have huge inventory fluctuations that impact its operations.\textsuperscript{117} Pharming is the exploitation of vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website’s traffic to another web site.\textsuperscript{118} Junk or spam web sites typically appear on search results and they do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, paste their names on open web forums and redirect traffic to known spammers.\textsuperscript{119}

\textsuperscript{114} e-Mail Spoofing: e-mail spoofing involves sending messages from a bogus e-mail addresses to e-mail address of other users. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP (Simple Mail Transfer Protocol), which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message. Retrieved from <http://www.techterms.com/definition/spoofing> visited on 15 December, 2012.

\textsuperscript{115} IP Spoofing: This involves masking the IP address of a certain computer system. By hiding or faking a computer’s IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions. Retrieved from <http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm> visited on 16 December, 2012.

\textsuperscript{116} Such as an online user name. For example, when posting on web discussion board, a user may pretend he/she is the representative for a certain company, when he/she actually has no association with the organization. In online chat rooms, users may fake their age, gender and location.


\textsuperscript{118} DNS servers are the machines responsible for resolving Internet names into their real addresses - the “signposts” of the Internet. Retrieved from <http://cyberlawsindia.net/Internetfraud.html> visited on 3 May, 2013.

\textsuperscript{119} id.
6.6.5 ATM Frauds

6.6.5.1 ATM Trapping

Trapping is simple and common fraud. Thieves do not need the credit/debit/smart card or the data. Thieves fix a device that causes notes to get stuck inside the dispensing machine. There is no way that the card-holder can know about the device from just looking at the machine outside. When the notes get stuck, the customer probably walks away to complain. The thieves keep a watch. When enough number of customers has walked in to withdraw, they come in and ‘clean’ the ATM. The customer walk away to another ATM without knowing that amount (mentioned for withdrawal in ATM machine) has been deducted from his/her amount because he/ she has not got that. Trapping also has resulted in a loss of millions of Euros in Europe alone.\(^\text{120}\)

6.6.5.2 Operational Fake ATMs

Fraudsters insert magnetic card reading equipments in ATM machine and a hidden mirror opposite to key pad. Sometimes a tiny spy cam is hidden to record the PIN. These magnetic card reading equipments steal data from credit cards and ATM cards. Customers try to withdraw money from these fake ATMs discover that the ATM does not work and walk away to another ATM. In the mean while, the equipment fitted with the ATM, records the data from the cards. The fraudsters now have access to the card details alongwith the PIN for these cards.\(^\text{121}\)

6.6.6 Unwanted Program- Adware, Spyware, Browser Parasites

The e-Commerce security environment is challenged by unwanted programs such as Adware, Browser parasites, Spyware and other applications that install themselves on a computer, typically without the users’ informed consent. Such programs are increasingly being found on social networking and user-generated content sites where users are befooled into downloading them. Once installed, these applications are usually difficult to remove from the computer.\(^\text{122}\) Adware is a new type of software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the advertisements, which can be

---

\(^\text{120}\) Rupa Mehta and Rohinton Mehta, 2009, p. 152.
\(^\text{121}\) ibid., p. 153.
viewed through pop-up windows or through a bar that appears on a computer screen. The justification for Adware is that it helps to recover programming development cost and helps to hold down the cost for the user. Adware is typically used to call for pop up ads to display when the user visits certain sites. Adware is not typically used for criminal activities. Zangosearch and Purity scan are examples of Adware programs that open the web pages or display pop-up ads of partner sites when certain keywords are used in the Internet searches.\(^\text{123}\)

A Browser Parasite is a program that can monitor and change the settings of a user’s browser, for instance, changing the browser’s home page, or sending information about the sites visitors to a remote computer. Browser parasites are component of Adware and steal personal information from victim’s computer. For example, Websearch is an Adware component that modifies Internet explorer’s default home page and search settings.\(^\text{124}\) Spyware is a technology that aids to gather information about a person or organization without their knowledge. Spyware gets into a computer as a software virus by installing a new program. Data collecting programs that are installed with the user’s knowledge are not, properly speaking, Spyware, if the user fully understands what data is being collected and with whom it is being shared. However, spyware is often installed without the user’s consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window. Spyware can be used to obtain information such as user’s keystrokes, copies of e-mail and instant messages, and even take screenshots that capture passwords or other confidential data.\(^\text{125}\) The latest scam to hit the headlines is the multi-million rupees Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated.\(^\text{126}\)

6.6.7 Hacking and Cybervandalism

A hacker is an individual who intends to gain unauthorized access to computer systems. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent; however both terms are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of websites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use. Sometimes hackers and crackers are satisfied merely by breaking into the files of an e-Commerce site. Others have more malicious intentions and commit Cybervandalism. Cybervandalism means intentionally disrupting, defacing or even destroying sites.\textsuperscript{127} Groups of hackers called “tiger teams” are sometimes used by corporate security departments to test their own security measures. By hiring hackers to break into the system from outside, the company can identify weaknesses in the computer system’s armor. These “good hackers” are known as “white hats” because of their role in helping organizations and fix security flaws. In contrast “Black hats” are hackers who break into websites and reveal the confidential information they find. Somewhere in the middle are “Grey Hats”; hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. “Grey Hats” discover weaknesses in a system’s security, and then publish the weakness without disrupting the site or attempting to profit from their findings. Hacking of bank accounts during online banking is one of the most common threats.

6.6.8 Malicious Code: Worms, Trojan Horses and Bots

Viruses, Worms, Trojans and Bots are part of a class of software called malware. Malware or malicious code (malcode) is short term for malicious software. It is code or software that is specifically designed to damage, disrupt, steal or in general inflict some other “bad” or “illegitimate” action on data, hosts or networks.\textsuperscript{128} Malicious code in the past often was intended simply to impair computers, and it was often authored by a hacker, but now-a-days the intent is to steal e-mail addresses, log in credentials,

\textsuperscript{127} Robert Lyttle of San Francisco and Benjamin Stark of St. Petersburg, Florida, were convicted of breaking into and “hacking” a computer at NASA’s Ames Research Center in Moffett Field, California. They state information about members of the agency’s Astrobiology Institute and used that information to deface the home page of the NASA Astrobiology institute.

presented data and financial information. Presently malicious code is used to develop integrated malware networks that organize the theft of information and money from banking institutions. Malicious Code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.\textsuperscript{129}

A virus is a computer program that has the ability to replicate or make copies of it and spread it to other files. In addition to the ability to replicate, most computer viruses deliver a ‘payload’. The payload display a message which may be highly destructive—destroying files, reformatting the computer’s hard drive or causing programs to run improperly. One of the latest innovations in virus distribution is to embed them in the online advertising chain, including at Google and other ad-networks. Worm is a malware that is designed to spread from computer to computer instead from file to file. A worm does not necessarily need to be activated by a user or program in order to replicate itself.\textsuperscript{130}

A Trojan horse is an email virus usually released by an email attachment. If opened, it scours hard drive for any personal and financial information such as social security account and PIN numbers. Once it has collected personal sensitive information, it is sent to a thief’s database. A Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious codes such as bots. Now-a-days, a Trojan horse hides a program to steal passwords and e-mail these passwords to hackers.\textsuperscript{131} Bots (short for robots) are a type of malicious code that can be covertly installed on one’s computer when attached to the Internet. Once installed, the bots responds to external commands sent by the attacker, and one’s computer becomes a “Zombie”, and is able to be controlled by an external third party (the “bot-herder”).


\textsuperscript{130} Computer worms are similar to viruses that replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. A worm enters a computer through vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. Retrieved from <http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html> visited on 15 December, 2012.

Botnets are collection of captured computers used for malicious activities such as sending spam, stealing information from computers and storing network traffic for later analysis.\textsuperscript{132}

\textbf{6.6.9 Salami Attacks and Jias Virus}

In addition to these, Salami attacks are used for committing financial crimes. In this financial crime the alteration in finances is so insignificant that in a single case it would go completely unnoticed. For instance, a bank employee or hacker inserts a program, into the banker’s servers, that deducts a small amount of money (40 Paisa per month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee or hacker will make a sizeable amount of money every month. The attack is called “salami attack” as it is analogous to slicing the data thinly, like salami. Salami attacks are covered by section 477-A\textsuperscript{133} of the IPC relating to falsification of accounts and Section 66 of the IT Act. But this fraud is very difficult to prove because of perpetrators programming. Moreover, recently \textit{JiasVirus} is very popular. This virus attacks financial accounts of online users particularly on facebook. It activates at the moment anyone clicks on the link and wait till it steals sensitive information.\textsuperscript{134}

There is a rising tide in the occurrence of banking frauds. In most cases, banks are unable to explain how each loss occurred, concluding that the most likely cause was malicious software secretly installed. In the light of strict regulatory controls, frauds are committed by increasingly sophisticated methods. Some of signs of such frauds are as under:\textsuperscript{135}

\begin{itemize}
\item [(a)] Unexpected charges on account;
\item [(b)] Credit report showing accounts which do not belong to the customer and contain inaccurate information;
\end{itemize}

\begin{flushright}
\textsuperscript{133} Making alteration in additions of any electronic entry in the bank’s computers would bring the offender within the ambit of Section 477-A of Indian Penal Code, 1908. This is also covered by section 66 of the IT Act where under any destruction or deletion or alteration of any information residing in computer resource or diminishing its value or utility or affecting it injuriously so as to cause wrongful loss or damage to the public or any person would be an offence.\textsuperscript{134}
\textsuperscript{134} The \textit{Amar Ujala}, Dehardoon Newspaper, 15 June, Saturday, 2013, p. 24.
\end{flushright}
(c) Bills and statements are still received even after mail stops arriving. This may indicate an identity of thief who has taken over the account and changed the billing address;

(d) Banking statements showing transactions which are significantly out of order;

(e) Receiving of credit cards without applying for them;

(f) Receiving of notice that you have been denied credit which was not applied;

(g) Receiving of calls or letters from debt collectors etc.

Scams are not only limited to the Internet transactions. Criminals also use phone and e-mails to gain personal information and commit fraud and identity theft. Some of the typical identity theft scams are: 136

(a) Notification by phone, e-mail or letter that you won a prize or lottery, but that person does not remember entering it at any point of time.

(b) Request to pay money in advance for service charges or taxes prior to receiving a prize or winnings.

(c) Promise to receive a huge sum of money in return for using particular website and bank account to send or receive money.

(d) Promise to make extra money working at home in return for using your bank account to send or receive money.

(e) Notification to pay a fee in advance to stop foreclosure, modify a loan or receive advice from a company or individual to stop paying mortgage.

(f) Notification to pay the travel money for attending the interview for some post which will be reimbursed later.

6.7 Judicial response to Online Banking or e-Banking frauds in India

The intensive use of Internet for e-Commerce, cyber marketing and commercial transactions-related communications have given rise to a number of fraudulent activities for which a person is held criminally liable. The judicial response to such cyber fraud is discernible from the leading Indian judgments handed down by the courts from time to time.

136 id.
The *Sony-Sambandh.com* (2002) was the first cyber-related fraud case in which the accused was convicted. This case has sent out a message that the provisions of the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act, 2000. The complainant Sony India Private Ltd. which was running a website called www.sony.sambandh.com. It enabled non-resident Indians to send Sony products to their relatives and friends in India after they make online payment for the products. In May 2002, someone logged on to the website under the identity of Ms. Barbara Campa and ordered a Sony coloured TV set and a cordless headphone. She gave her credit card number for payment and requested the product to be delivered to Arif Azim in Noida. The payment was cleared by the complainant Sony India Ltd. who delivered the items to Arif Azim after following the relevant procedure of due diligence. It also took a digital photograph showing the delivery being accepted by Arif Azim. Nearly one and a half month after this transaction, the credit card agency informed Sony (India) company that it was an unauthorized fraudulent transaction as the real power had denied having made the purchase. Thereupon, the company lodged a complaint for online cheating to the CBI which registered a case against Arif Azim under Sections 418, 419, 420 of the Indian Penal Code. The investigation of the case revealed that the accused Arif Azim who was working at a call center at Noida gained access to the credit card number of an American national, which he had misused on the company’s website. The CBI recovered the coloured TV and cordless head phone from Arif Azim. The Court on the basis of evidence of witnesses and material before it found Arif Azim guilty of offences under Sections 418, 419, 420, IPC and convicted him for cyber fraud and cheating. However, in view of the young age of the accused i.e. 24 years and this being his first conviction, the Court ordered his release on probation for a period of one year.¹³⁷

In the *Pune Citibank Fraud* case¹³⁸ four US customers were defrauded to the tune of 3.5 lakhs US dollars which were transferred by the fraudsters to bogus accounts. This case

---


is related to outsourcing of engineering services. Some employees gained the confidence of the customers and acquired their PIN numbers and passwords to commit the fraud. MphasiS, a call center hired the services of former Citibank executives to assist it in obtaining and implementing City Bank outstanding contracts in 2002. The defrauded customers complained that all fake accounts were opened in Pune and the money from their account was transferred to Pune account. The police in Pune claimed that after intensive raids and checks in the call centers, cyber cafés and interrogation of employees working there, they were convinced that the employees had no involvement in the fraud and their services were reliable. The police had also frozen the accounts in which the money was transferred. One of the MphasiS official in India Shri Vivek Dayal on December 1, 2005, in a reply to an e-mail enquiry about progress of investigation in the case informed MphasiS in US that he regrets that some ex-employees seemed to have been involved in this fraud. However, the initiative taken by the police and the investigating authorities successfully traced the culprits. The investigation in the case revealed that all eleven accused were involved in the fraud including three ex-employees of the MphasiS and the other eight were not the employees of MphasiS. There three ex-employees were the customer service agents who came into contact with four US customers who called into MphasiS call center for help with their Citibank accounts. The three ex-employees culprits gained the confidence of these unfortunate victims and obtained their PIN numbers and other account details, which they used to transfer money from victim’s account into the accounts of members of the fraud gang. The three were working at MphasiS call center for six months. The fraud was discovered by the customers who notified it to the Pune Citibank and reported the case to the police. As a result, it was made mandatory that there is need for national ID and a national data base where a name can be referred to. Customer education is very important so that customers do not get taken for a ride. Most banks are guilty of not doing this.  

---

139 The eight arrested accused persons other than the three ex-employees of MphasiS were: S.C. Burewar, Ginny George, Nitin Valkar, Vijay More, P. Philippose, S. Ramanujam, Satish Parab and Bijoy Alexender. All of them were in the age-group of 23 to 30 years except Nitin Valkar who was 42 years of age. The case is still under judicial scrutiny.

In yet another case, i.e. *Infinity e-Search (Gurgaon BPO)*, a young person Karan Bahari aged 24 years was working for a Gurgaon based website designing and online marketing firm Infinity e-search. He was alleged to have fraudulently sold information of 1000 bank accounts of British customers from an Indian call center to an undercover British journalist working for a British newspaper, *The Sun* for 2750 pounds. The employee Karan, however, denied the charge and claimed that he was only a middleman and that he did not sell data collected by his employer i.e. Infinity e-search company. The company also denied any involvement in the case. In this case, it was alleged that the British journalist for “*The Sun*” used Karan Bahari who was working in the Infinity e-search, as an intermediary, offered him a job and requested for a presentation on a CD and later claimed that the CD contained confidential data about thousand Bank accounts of British customers who were customers from an Indian call centers. However, on investigation, the fact that the CD contained such data could not be substantiated by the journalist and, therefore, the charges of fraud could not be proved against Karan Bahari or his employer i.e. The Infinity e-search company. But the case has raised an apprehension that there is possibility of an anti-outsourcing backlash if Indian online companies do not take sufficient care of the data which they handle.

The Supreme Court’s ruling in the *Morgan Stanley’s case* has been instrumental in augmenting Business Processing Outsourcing (BPO) with a view to create a global safe-deposit vault to halt data theft and improve India’s prospects on outsourcing destination. The National Association of Software and Services Companies (NASSCOM) announced setting up of an independent watchdog Self Regulatory Organization (SRO) in April, 2007 for setting out data security standards for the software industry with focus on global practices.

In the context of online frauds, the notorious *World Wide Nigerian Scam* deserves a special mention. This scam is better known as Advance Fee Fund (AFF) or Nigerian Fraud or the ‘419 Fraud’. The ‘419 Fraud’ is named after Section 419 of the Criminal

---

141 Decided by Delhi High Court on June 24, 2005.
Code of Nigeria, which is operating in most of the European and Anglo-American countries since 1980’s has duped the business world to the tune of Billions of US Dollars. It is reported to be the fifth largest industry in Nigeria operated by unscrupulous business elites under the successive Governments of that country. The modus operandi of the scam is as follows: The victim (target) receives an unsolicited fax, e-mail or letter concerning Nigeria or any other African nation, mostly from West Africa such as Ghana, Togo, Liberia, Sierra, Leone, Ivory Coast etc; requesting for legal and legitimate business proposal or service contracts. The victim is asked to pay an advance fee of some kind which may be in the form of ‘transfer tax’, ‘performance bond’ or for ‘credit privileges’. Once the victim pays the fee, many more requests for advance payments on one pretext or another come to the victim until he/she either decides to quit or runs out of money, or both. The moment victim gives his/her account details, he/she has to suffer a huge amount of financial loss.

Alarmed by the widespread Nigerian ‘419 Fraud’ the Government of USA, UK, Canada, South Africa etc., have warned the business community to be alert and not to respond to 419 letters, instead file a complaint against the sender with the national law enforcement agency and also to Nigerian Embassy and the Central Bank of Nigeria. Those who have fallen a pray to such scam may also file a complaint with the Nigerian Economic and Financial Crimes Commission. An International Working Plan to combat this ongoing Nigerian criminal activity has been suggested by the G-8 countries along with Russia in 1996. As a concerted effort to end this menace the United States with 38 other Governments who raised the issue of 419 Fraud with the Nigerian Government to initiate stringent measures against those involved in this trans-national scam.

In United States vs. Pirello, the defendant placed four fraudulent advertisements on classified-ads websites, soliciting buyers for computers. He received three orders for the purchase of computers in response to the said web-advertisement and obtained price money which he deposited in his personal bank account but never delivered the computers to the buyers. On complaint from the cheated victim, Pirello was tried for the

144 Vishwanath Paranjape, 2010, p. 140.
145 The G-8 countries joined by Russia met in Lyon (France) in 1996 and expressed serious concern for this transnational Nigerian cybercrime.
146 (2001) 12 255 F. 3d. 728 (Ninth Circuit Court).
offence of Internet fraud and the trial court sentenced him with enhanced punishment by two levels as per U.S. law, as the offence was committed through ‘mass-marketing’ by resorting to fraudulent Internet advertisement. On appeal, the Court of Appeal upheld the enhanced sentence and declined to interfere with the decision of the lower Court.

One of the important cases was ICICI Bank Phishing case. E-mails, that is considered as the most convenient form of communication, can bring some shocking surprises. Recently, few ICICI Bank customers in Mumbai, to their utter dismay, discovered that e-mails can be extremely hazardous, if not to their health, at least to their security. These customers received an e-mail from someone who himself/herself posed as an official of the bank and asked for sensitive information like Internet login name and password of the account holder and directed them to a web page which resembled with the official site page of the bank. The e-mail seemed so genuine that some users even clicked on the URL given in the mail to a web page that resembled the official site. When some customers wrote and asked to find out the purpose of the e-mail, the bank officials were left with no option except to register a complaint with the police. Such a scam is known as ‘phishing.’ It is actually a banking scam and a warning against which had been issued by many International banks including Citibank.147

Another relevant fraud is Cyber Lotto as a Tool for Frauds. It was a classic case of Cyber crime and the first of its kind in Andhra Pradesh. A newspaper in Hyderabad has received an email that KVK Mohan had won the Euro lottery. The website address was given for verification. The newspaper sent the query and got the confirmation since KVK Mohan had himself created and manipulated the website. The case was investigated by Shri Sudeep Lakhtakia, Police Commissioner of Vijaywada. In fact a case of cheating and fraud was registered against one Kola Venkata Krishna Mohan, the self-styled winner of the multi-million dollar Euro lottery. He admitted that he did not win the 12.5 million pound Euro lottery as he had claimed. He has merely played fraud to make good his losses in gambling. With the help of computers, the accused took the people for a ride. The Police Commissioner of Vijaywada pointed out that Mohan by

using the Internet had forged documents, cheated banks and several persons to the tune of 60 million rupees. KVK Mohan was arrested for fraud and forgery and was sent in judicial custody. Mohan was accused of cheating Andhra Bank of ₹ 1.73 million. He was a gambler and played cards regularly at high stakes in various clubs. He told media that he had lost ₹ 30 million in 1998 when a gambling syndicate led by a real estate dealer and a restaurant-owner cheated him.\footnote{Alok Mishra and K.B. Asthana, July, 2012, pp. 82-100 at p. 95.}

In another *Criminal abuse of debit cards* case three persons, including a security guard deployed at an ATM outlet in Paharganj, Delhi were arrested for allegedly duping over 200 people by obtaining details of their debit cards on the pretext of helping them and using the proceeds to buy air and railway tickets online. They were active for about six months and duped people of ₹ 6 Lakh as per police investigation. The fraud came to light when a man approached the crime branch of Delhi Police mentioning that ₹ 42,682 had been withdrawn illegally from his State Bank of India account by abiding his debit card online. Investigations revealed that the complainant had withdrawn some cash from the SBI ATM in Paharganj a month ago and had taken the help of the security guard deployed there during the transaction. Acting on the information, the police arrested security guard Mohinder Sharma and his accomplice Ajit Singh, a Commerce graduate. Their third accomplice, Anil Mehra was arrested later at their instance. The police claimed to have recovered about 250 Debit card numbers and their respective Personal Identification Numbers from their possession. It was revealed during investigation that Ajit Singh, a resident of Ghaziabad in Uttar Pradesh, became friend with Mohinder six months ago when he came to stay at a hotel in Paharganj and was impressed by the memory of the security guard who could memorise long numbers. The two then hatched a conspiracy to abuse the capability of the guard to memorise numbers to get the details of the debit cards of people coming to the ATM booth. Mohinder used to memorise the debit card number on the pretext of helping those who came to the ATM booth and also observed them typing the PIN. He could send the details to Ajit for ₹ 500 per card and made ₹ 1.25 Lakh. Anil Mehra, who belonged to Amritsar, found customers willing to buy air and railway tickets and got them booked through Ajit using
the card details. Ajit charged 60 per cent of the actual cost of the tickets from Anil who further sold it to customers at a price lower than the actual price.\textsuperscript{149}

On 12 April, 2010, a landmark judgment of \textit{S. Umashankar Sivasubramanian vs. ICICI Bank} came out of the office of the Adjudicating Authority of Tamil Naidu under Information Technology Act, 2000 at Chennai\textsuperscript{149} the complainant alleged that his account was wrongfully debited due to negligence on the part of the bank. ICICI contended that the case refers to phishing and the blame of negligence lies with the customer who would need to file an FIR and also raised a preliminary objection that the matter cannot be brought under the purview of IT Act. The Adjudicating Authority however vide its decision dated 12.04.2010 stated that ICICI bank had failed to establish that due diligence were exercised to prevent the contravention. ICICI Bank was found guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act, 2000 and directed the ICICI to pay a total sum of \textsterling 12,85,000/- (which includes an amount of \textsterling 6,00,000 towards expenses). ICICI bank has obtained a stay on the judgment (upon depositing \textsterling 50,000) in an appeal filed by them before the Cyber Appellate Authority.\textsuperscript{150} This judgment was decided with reference to the IT Act, 2000 and not the IT Act, 2008 because this case occurred in September, 2007 at that time when the IT Act, 2008 was not in place.

\textit{Avnish Bajaj vs. State}\textsuperscript{151} was decided by the Delhi High Court in which it discussed the criminal liability of a network service provider being Baazee.com for third party data or information made available by them on their site. Argument of the prosecution was that the accused did not stop payment through Banking channels after learning of illegal nature of transaction. The Delhi High court has held that “on a conjoint reading of Section 67 and 85 of the Information Technology Act, 2000, it may be concluded that on the basis of the principle of deemed criminal liability, a case may be made out against any director of a company even though the company may not be arrayed as an accused provided the ingredients laid down in the section are satisfied”. This judgment did not declare Avnish Bajaj guilty.

\begin{flushright}
\footnotesize\textsuperscript{149} ibid., p. 96.
\textsuperscript{151} (N.C.T.) of Delhi (2005) 3 Comp. L.J. 364 (Del.).
\end{flushright}
National Association of Software and Services Companies vs. Ajay Sood and Others\textsuperscript{152} case was a reasoned order approving a settlement agreement between the plaintiff and the defendants in a case which dealt with the issue of ‘phishing’, wherein a decree of 16 Lakh was passed in favour of the plaintiffs. It is the contention of the plaintiff that the defendants were masquerading as NASSCOM, and were sending emails, in order to obtain personal data from various addresses, which they could then use for financial gains, and they went on the website as if they were a premiere selection and recruitment firm. The suit was filed praying for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent e-mails purportedly originating from the plaintiff of using the trade mark ‘NASSCOM’ or any other mark confusingly similar in relation to goods or services. The Hon’ble Judge further observed that “I find no legislation in India on ‘phishing’. An act which amounts to phishing under the Indian law would be a mis-representation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even the person whose name, identity or password is misused. It would also be an act of passing off as is affecting or tarnishing the image of the plaintiff, if an action is brought by the aggrieved party.”

In ICICI Bank vs. Ashish Agrawal\textsuperscript{153} case the appeal was filed against the order dated 27.07.2009 of the District Consumer Disputes Redressal Forum, Raigarh directing the appellant bank to pay ₹49,912.36, which was allegedly not withdrawn by him from his account and also ₹5,000 as compensation for mental agony and ₹3,000 as litigation cost to the respondent/complainant on account of deficiency in service, regarding maintenance of his bank account. The complaint was filed alleging deficiency of service on the part of the appellant bank as rupees ₹49,912.36 was withdrawn from his bank account, without his knowledge, using Internet banking. The State Commission vide its order dated 26.03.2010 allowed the appeal. The Commission observed that the respondent was negligent in giving information regarding password to a third person


and hence deficiency of service could not be attributed on the part of the appellant bank, who had taken all precaution to give every instruction to the customer and also authorized him to change his password as and when desired.

In the case of *Rishi Gupta vs. ICICI Bank Ltd.*, the complainant alleges that an amount of ₹3,00,000 was transferred from his account fraudulently through 15 transactions of ₹20,000 each. The District Forum vide order dated 21.06.2010 dismissed the complaint. The Hon’ble court in its order observed that in providing confidential details of his online banking such as corporate ID, password etc., to a third party in response to an email purported to be issued by the opposite party bank, without verifying with the opposite party bank, the complainant had acted negligently and he cannot put the blame on the bank.

In *M/s Pachisia Plastics vs. ICICI Bank Ltd.* case the complaint was filed alleging deficiency of service on the part of opposite party (Bank) on the ground that an amount of ₹1,18,000 was debited from the account of the complainant through net banking without his authorization. The Forum vide order dated 11.07.2009 dismissed the complaint on the ground that there was no deficiency of service on the part of the bank. In the order dated 11.07.2009, it was observed that the burden lies on the complainant to establish that he has kept the code number (password for net banking) secret and that there appeared to be a carelessness and negligence on the part of the complainant.

In *K. Thagyarajan vs. ICICI Bank* case the complainant alleged that his Internet bank account was breached and an amount of ₹77,000 was unlawfully transferred to another account by some unknown persons. The complainant has alleged deficiency of service on the part of the opposite party bank and prayed for refund of the amount with interest and ₹3,00,000 to be awarded as compensation. The complaint was dismissed vide order dated 20.05.2010 on the ground that there was no deficiency of service on the part of

---


opposite party bank as the complainant had himself delivered the password and user id (for Internet banking) to others.

In *Smt. Vimala Varkey & Others vs. HDFC Bank Ltd. & Others* the complainant was aggrieved that money was fraudulently transferred from her account maintained with opposite party No. 1 Bank to an account maintained with opposite party No.2 Bank (ICICI Bank). The complainant alleged deficiency of service by opposite party No.1 Bank and had prayed for reimbursement of the amount with interest. It was observed that the complainant had, admittedly, herself disclosed her customer ID & PIN to a third party, in reply to a phishing mail and on the basis of such information the third party might have managed to transfer the amount. The terms and conditions, of opposite party No.1 Bank, governing operation of Net Banking, stipulated that opposite party cannot be held responsible for the loss sustained by the complainant in such transactions. The Forum, therefore, dismissed the complaint vide its order dated 2.09.2008 on the ground that there was no deficiency of service on the part of the opposite party bank. Therefore, it is need of the time to balance the interests of customers and that of banks and provide protection to banks against any fraudulent or negligent act of customer.

It has been observed that Indian judiciary is taking strong steps against newly emerged e-Banking frauds. These decisions of the hon’ble courts provide a sound ground for the growth of stringent provisions in cyber law against online financial frauds. In addition to this, the G. Gopalakrishna Working Group on Electronic Banking has also given several recommendations for safe electronic banking in its report. However, it is need of the time to make some amendments in the Information Technology Act, 2000 (2008) and add penal provisions for the offences against consumers during e-Banking transactions. The following pages depict the legal control mechanism to combat frauds in e-Banking from which it is crystal clear that in Indian Cyber Jurisprudence, it is very important to enact strict penal as well as compensatory provisions.

---

6.8 Legal Control Mechanism to combat frauds in e-Banking in India: An Overview

6.8.1 Influence of International Instruments on Indian Law

The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. In many countries, Constitutions reflect this right to Privacy. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in Germany in 1970. This was followed by National laws in Sweden (1973), the United States (1974) and in France (1978). Two crucial International instruments evolved from these laws i.e. the Council of Europe’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Organization for Economic Cooperation and Development’s (OECD) guidelines governing the protection of privacy and trans-border data. Flow of Personal Data articulated rules covering the handling of electronic data. The rules within these two documents from the core of the data protection laws of several countries. These rules describe personal information as data which is afforded protection at every step from collection to storage and dissemination. The right of people to access and amend their data is a primary component of these rules. The expression of data protection in various declarations and laws varies. All that is required is that the personal information must be obtained fairly and lawfully, it must be used only for the original specified purpose for adequate and relevant objective and must be destroyed after its purpose is completed. These two agreements have had a profound impact on the adoption of laws around the world including India. The OECD guidelines have also been widely used in other national legislations, even outside the OECD countries.\textsuperscript{158} Several principles of data protection are strengthened under the Directives, namely the Right to know from where the data is originated, the Right to have inaccurate data rectified, Right to recourse in the event of unlawful processing and the Right to withhold permission to use data in some circumstances.\textsuperscript{159}

\textsuperscript{158} Alok Mishra and K.B. Asthana, July, 2012, pp. 82-100 at p. 84.
\textsuperscript{159} K. Nageswar Rao, Bank Credit-Emerging Trends, ICFAI University Press, Nagarjuna Hills, Punjagutta, Hyderabad (India), 2002, pp. 91-98.
Since personal information is a manifestation of an individual personality, the Indian courts including the Supreme Court of India, have recognized that the Right to privacy as an integral part of the Right to life and personal liberty, which is a fundamental Right guaranteed to every individual under the Constitution of India. Presently, there is no specific legislation dealing with privacy and data protection. The protection of privacy and data can be derived from various laws pertaining to Information Technology Act, Crimes, Intellectual property, and Contractual relations. The law laid down in Tournier’s case is followed in India in the case of Shankarlal Agarwalla vs. State Bank of India also and banks are required to maintain secrecy of the accounts of their customers. The exceptions to the rule are as under: (a) where the disclosure was under compulsion by law, (b) where there was a duty to the public to disclose, (c) where the interest of the bank requires disclosure and (d) where the


161 The Information Technology Act provides for safeguard against certain breaches in relation to data from computer systems. The said Act contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein.

162 The Indian Penal Code, 1908: The Indian Criminal law does not specifically address breaches of data privacy. Under the Indian Penal Code, liability for such breaches must be inferred from related crimes. For instance: Section 403 of the India Penal Code imposes criminal penalty for dishonest misappropriation.

163 The Intellectual Property Laws: The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison. Fines are also prescribed.

164 The Credit Information Companies Regulation Act, 2005 (“CICRA”): As per the CICRA, the credit information pertaining to individuals in India have to be collected as per privacy norms enunciated in the CICRA regulation. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. Based on Fair Credit Reporting Act and Graham Leach Bliley Act, the CICRA has created a strict framework for information pertaining to credit and finances of the individuals and companies in India. The CICRA has created a strict framework for information pertaining to credit and finances of the individuals and companies in India. The Regulations under CICRA which provide for strict data privacy principles have recently been notified by the Reserve Bank of India. For additional knowledge see: The Financial Modernization Act of 1999, which is also known as the ‘Gramm-Leach-Bliley Act’ or GLB Act. It includes provisions to protect consumers’ personal financial information held by financial institutions. Manjula Chawla, “Overview of Data Protection Laws in India”, Retrieved from <http://www.ehcca.com/presentations/privacysymposium1/steinhoff_2b_h1.pdf> visited on 10 January, 2013.


166 Shankarlal Agarwalla vs. State Bank of India and Others. AIR 1987 Cal. 29.
disclosure was made by express or implied consent of the customer. The Personal Data Protection Bill, 2006 and the Privacy (Protection) Bill, 2013 are introduced in Parliament for protection of personal data. The use of technology in the field of banking appears to have thrown up fresh challenges to banks in fulfilling their obligation to maintain the relationship of banker and customer under the guidelines of the courts.

6.8.2 Negotiable Instruments Act, 1881
Under Negotiable Instrument Act 1881, cheque includes electronic image of truncated cheque and a cheque in the electronic form. The truncation of cheques in clearing has been given effect to and appropriate safeguards in this regard have been set forth in the guidelines issued by RBI from time to time. A cheque in the electronic form has been defined as “a mirror image” of a paper cheque. The expression ‘mirror image’ is not appropriate. It is perhaps not even the intention that a cheque in the electronic form should look like a paper cheque as seen in the mirror. Further, requiring a paper cheque being written first and then its mirror image or electronic image being generated does not appear to have been contemplated as the definition requires generation, writing and signature in a secure system etc. The expression “mirror image” may be substituted by the expression, “electronic graphic which looks like” or any other expression that captures the intention adequately. The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year 2002, it is understandable that it has captured only digital signature and asymmetric crypto system under Section 3 of IT Act, 2000. Since IT Act, 2000 has been amended in the year 2008 to make provision for electronic signature also, suitable amendment in this regard are required in NI Act, 1881 so that electronic signature may be used on cheques in electronic form.

6.8.3 Prevention of Money Laundering Act, 2002 (PMLA) & PML Rules
Under section 12 of PMLA, 2002 every banking company, financial institution and intermediary, as the case may be, is required to maintain a record of transactions as may be prescribed by rules and furnish information to the Director within such time as may

---

168 id.
be prescribed. The records to be maintained by such entities are set forth in rule 3 of PMLR, 2002. Such records include record of cash transactions of value more than 10 lakhs or its equivalent in foreign currency, integrally connected cash transactions taking place within a month, cash transactions where forgery or counterfeit notes are involved and suspicious transactions of the nature described therein. Under rule 6 of PMLR, 2002 such records are to be maintained for a period of ten years from the date of transaction. The period before which the transactions have to be reported to the Director are set forth in rule 8 of PMLR, 2002. With respect to the transactions of 10 lakhs and more and the integrally connected transactions referred to above, the information has to be submitted every month before the 15th day of the succeeding month. The information relating to forged or counterfeit notes is required to be submitted within seven days of the date of occurrence of the transaction. As regards suspicious transactions, principal officer of such entities is required to furnish the information in writing or fax or email to the Director within a period of seven working days on being satisfied that the transaction is suspicious. The requirement of maintaining the records by such entities regarding the identity of their clients is prescribed in rule 9 of PMLR, 2002.

Though the above requirements under PMLA and PMLR appear to be procedural in nature, it needs to be appreciated that the maintenance of records and reporting of transactions help in tracking transactions involving money laundering or the persons involved in such transactions. Under section 13 of PMLA, 2002 the Director is empowered (without prejudice to take any other action under PMLA) to impose a fine which shall not be less than ten thousand but which may extend to one lakh for each failure. In terms of Section 70 if the contravention is committed by such entities the officers in charge of and responsible to the conduct of the business of such entity at the relevant time are also liable to be proceeded with and punished. It is therefore clear that such entities should have a robust system of keeping track of the transactions of the nature referred to in PMLA, 2002 and PMLR, 2002 and report the same within the prescribed period as aforesaid. Apart from the risk of penalty, this involves reputational risk for such entities.\(^{169}\)

\(^{169}\) id.
6.8.4 The Payment and Settlement Systems Act, 2007 (PSS Act)

In India prior to 2007, there was no enactment which dealt with the issue of Electronic Fund Transfer. The Payment and Settlement Systems Act, 2007 (PSS Act) has been enacted in 2007 and the directions as well as guidelines are issued there under to deal, to a certain extent, with this issue. This PSS Act 2007 has been adopted under the influence of the Electronic Fund Transfer Act of USA.\(^{170}\) Section 2(1)(c) of PSS Act\(^{171}\) does not restrict itself to transfer of funds initiated through electronic means but deals with transfer of funds that are initiated by a person by other means and that are settled electronically. Therefore, it has brought Electronic Clearing System (ECS), auto-debit instructions etc. within its ambit. Section 18 of the PSS Act, 2007 empowers the Reserve Bank to issue directions and such directions issued by the Reserve Bank are compulsory to be complied with. The Act also prescribes the penalties/punishments for failure to comply with the provisions of the Act, rules, regulations, orders and directions issued there under. Section 25 of the Act deals with the issue of dishonor of Electronic Funds Transfer for insufficiency of funds and makes it an offence punishable with imprisonment for a term which may extend to two years or with fine or with fine which may extend to twice the amount of the electronic fund transfer, or with both. So as to make the process of electronic fund transfer more smooth and effective, the Reserve Bank has been issuing a number of guidelines to deal with the various aspects of and procedures for electronic fund transfer.\(^{172}\)

6.8.5 The Information Technology Act, 2000 and the IT (Amendment) Act, 2008

On 11 April 2011, the Indian Ministry of Communications and Technology published rules for implementing certain provisions of the Information Technology (Amendment)

---

\(^{170}\) In the USA the Electronic Funds Transfer Act (EFTA), 1978 read with the Electronic Fund Transfers Regulation (Regulation E) provides the basic framework establishing the rights, liabilities and responsibilities of participants in electronic fund transfer systems. The Electronic Fund Transfer Act, 1978 is basically a consumer protection measure and is codified as title IX of the Consumer Protection Act. Also see: <http://www.fdic.gov/ regulations/ laws/rules/6500-1350.html#fdic6500904> visited on 11 January, 2013.

\(^{171}\) Section 2(1) (c) ‘electronic funds transfer’ means any transfer of funds which is initiated by a person by way of instruction, authorization or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, Internet and card payment.

Act 2008 dealing with: (a) Protection of sensitive personal data: security practices and procedures that must be followed by organisations dealing with sensitive personal data (Data Privacy Rules); (b) Due diligence to be observed by intermediaries and (c) Guidelines for Cybercafés. Under the Information Technology (Amendment) Act, 2008 some of data protection provisions are as follows: Under Section 43-A, a body corporate that possesses, deals or handles ‘Sensitive Data’ in a computer resource is liable to pay compensation if it is negligent in implementing and maintaining reasonable security practices and procedures, and such negligence results in wrongful loss or wrongful gain to any person. Section 43-A fixes liability on a body corporate that is negligent in implementing security measures for the protection of ‘Sensitive Data’ and if such negligence results in wrongful loss or wrongful gain to any person. The Central Government has not prescribed the term ‘sensitive personal data’, whether it includes very personal information about Banking Accounts like: Account Number, PIN Number, Address, Mobile Number, Security Code and other such information. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law. However, Explanation (ii) to Section 43A is worded in such a way that there is lack of clarity whether it would be possible for banks, or anybody corporate to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide act on the part of the customer or any other stranger (hacker) would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extreme situations. The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs.

Apart from affording protection to personal data (sensitive personal data or information under section 43-A (iii), the Information Technology Act, 2000 also prescribes civil and

---

173 Section 43-A of the Information Technology (Amendment) Act, 2008 states Compensation for failure to protect data (Inserted vide ITAA 2006).

174 Also See: The case of Umashankar Sivasubramanian vs. ICICI Bank (Before the Adjudicating Authority under Information Technology Act, 2000 at Chennai.)
criminal liabilities (Section 43\textsuperscript{175} and Section 66\textsuperscript{176} of the Information Technology Act, 2000 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., inter alia, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. Under section 66 if any person does any act referred to in section 43\textsuperscript{177}, with dishonest and fraudulent intention, he shall be punished with the imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 66-C\textsuperscript{178} has been added with the Information Technology (Amendment) Act, 2008 to penalize the offence of Identity Theft. Section 66-D\textsuperscript{179} has been added with the Information Technology (Amendment) Act, 2008 to penalize cheating by Personation by using Computer Resource. In this context Section 72\textsuperscript{180} and 72-A\textsuperscript{181} of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record, book, register, correspondence, information, document or any other material etc. and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both. Section 72-A on the other hand provides the punishment for disclosure of personal/ confidential data by any person, including an intermediary, in breach of lawful contract. The purview of section 72-A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract by virtue

\textsuperscript{175} Section 43 of the Information Technology Act, 2000 explains Penalty for damage to computer, computer system, etc.

\textsuperscript{176} Section 66 of the Information Technology Act, 2000 entitled Hacking with computer system has been substituted with new Section 66 entitled Computer Related Offences.

\textsuperscript{177} Section 43 of the Information Technology Act, 2000 provides penalty and compensation for damage to computer, computer system, computer network, computer data base and many other computer related offences.

\textsuperscript{178} Section 66-C the Information Technology (Amendment) Act, 2008 prescribes punishment for identity theft (Inserted Vide ITA 2008).

\textsuperscript{179} Section 66-D of the Information Technology (Amendment) Act, 2008 states punishment for cheating by personation by using computer resource (Inserted Vide ITA-2008).

\textsuperscript{180} Section 72 of the Information Technology Act, 2000 provides provisions for penalty for breach of confidentiality and privacy.

\textsuperscript{181} Section 72-A of the Information Technology (Amendment) Act, 2008 states punishment for disclosure of information in breach of lawful contract (Inserted vide ITAA-2008).
of ‘powers granted under IT Act, 2000’. Under Section 72-A of the IT Act (introduced by IT Amendment Act 2008), a person who is providing services under a lawful contract, may be liable to imprisonment for a term of up to three years or a fine up to Rupees Five lakh for disclosure of personal information of any individual: (a) with the intent to cause, or knowing that he is likely to cause, wrongful loss or wrongful gain; and (b) without the consent of such individual, or in breach of lawful contract. The IT Act does not define ‘personal information’. It is however defined in the context of sensitive data under Section 43-A (iii) of the IT Act.\(^\text{182}\)

In India, till recently, there is no specific provision to address the issue of Data Protection. However, The Information Technology Amendment Act, 2008 has taken initiative in addressing the lacuna of data protection laws in the country. The provisions are, however, not adequate to meet the needs of the data protection in India.\(^\text{183}\) It has been observed by the researcher that the Bible of Cyber law is the Information Technology Act, 2000 (2008). Whenever any illegal act occurs in cyberspace, all eyes look upon the Information Technology Act, 2000 (2008) for solution. After a minute analysis of this Act, it is seen that most of the provisions are focused on disclosing of personal information and its punishment either by body corporate or otherwise. No mandatory protection has been provided against offences like Phishing, Pharming, Cyber Money laundering, ATM Frauds and other financial frauds wherein innocent consumers are cheated and defrauded. Guidelines provided by RBI are just precautionary measures. In order to make e-Banking safe and reliable, it is very important to add penal stringent provisions in the Information Technology Act, 2000 (2008).

\textit{6.8.6 Legal Protection provided by Reserve Bank of India (RBI) in e-Banking:}

The Reserve Bank of India (RBI) is India’s central banking and monetary authority. It was set up on April 1, 1935 under the Reserve Bank of India Act, 1934. RBI’s central office was initially in Kolkata but moved to Mumbai in 1937. RBI regulates businesses,


interest rate, price stability, fund raising activities for the Central and the State governments through the auction of government securities, manage currency exchange rates, supervise banks and non-banking financial institutions, regulate consumers, controls the availability of funds in the financial system for credit and loans offered by banks and non-banking financial institutions to government entities. Reserve Bank is also responsible for monitoring the foreign exchange flows into the Indian economy.\textsuperscript{184}

In the lap of Internet technology the tools of committing bank frauds have become highly sophisticated. An ordinary individual is not able to recognize that he has become victim of online frauds. Therefore, RBI issue guidelines as well as precautions from time to time for general public.

6.8.6.1 Guidelines Issued by Reserve Bank of India for General Public

Therefore, RBI has issued guidelines for the innocent public as under:

(a) RBI does not hold any accounts for individuals;
(b) Beware of impersonated names of RBI officials;
(c) Nobody from RBI calls up people about lottery winnings/funds received from abroad;
(d) RBI does not send any emails intimating award of lottery funds, etc.;
(e) RBI does not send any sms or letter or email to communicate fictitious offers of lottery winnings or funds received from abroad;
(f) The only official and genuine website of the Reserve Bank of India is (www.rbi.org.in) and the public must be careful and not get misled by fake website with similar addresses beginning with ‘Reserve Bank’, ‘RBI’ etc., along with fake logos; and

(g) Inform local police or Cyber Crime Authority about such frauds. The Reserve Bank of India has, on several occasions in the past, cautioned the members of public not to fall prey to fictitious offers/lottery winnings/ remittance of cheap

funds in foreign currency from abroad by so-called foreign entities/individuals or to Indian residents acting as representatives of such entities/individuals.\textsuperscript{185}

6.8.6.2 Precautions to be observed by public as highlighted by Reserve Bank of India

Describing the modus operandi of the online frauds, the Reserve Bank has stated that the fraudsters send attractive offers to gullible public through letters, e-mails, mobile phones, sms etc. To lend credence to such offers, the communication often sent on/from letterheads/websites that appear to be like that of some public authorities like the Reserve Bank of India. The offers are purportedly signed by top executives/senior officials of such authorities. While the names of the officials might be correct but their signatures are fake. The offer document would contain contract details of a so-called RBI officer working in some department in the Reserve Bank/public authorities.\textsuperscript{186} The fraudsters initially ask potential victims to deposit small sum of money for reasons, such as, processing fees/transaction fees/tax clearance charges/conversion charges and clearing fees etc. The victims are asked to deposit the money in a specified account in a bank. The fraudsters often have multiple accounts in the names of individuals or proprietary concerns in different bank branches for collecting such charges. Genuine but gullible account holders are persuaded by the fraudsters to even lend their accounts for such fraudulent activities on the promise of receiving some commission.\textsuperscript{187} Once the initial amount is deposited, demands for more money follow with more official sounding reasons. After accumulating a sizeable amount in these accounts, the fraudsters withdraw or transfer the money abroad and vanish leaving the victims in a lurch. Many residents have already become victims and have lost huge sums of money by falling for such fictitious offers. The public is advised to register their complaints with the local law enforcement agencies. In its Press Release the Reserve Bank has given some advices and the list of such nodal agencies with which the public can register complaints.\textsuperscript{188}

\textsuperscript{185} Alok Mishra and K.B. Asthana, July, 2012, pp. 82-100 at p. 97.
\textsuperscript{186} id.
\textsuperscript{187} id.
i) Complain to Local Police/Cyber Authorities against fictitious offers of money from abroad.

ii) RBI Never asks for your Bank Account details.

iii) Do not Pay Money to receive large funds from abroad.

iv) Do not fall prey to fictitious offers of funds transfer.

v) Remittance towards participation in lottery, money circulation schemes, other fictitious offers of cheap funds, etc.

vi) Beware of fictitious offers/lottery winnings/Cheap fund offers

vii) RBI cautions public against fictitious offers of remitting cheap funds from abroad

It can be mentioned here that regulations and guidelines made by the Government of India and Reserve Bank of India to check these types of problems should be strictly implemented. The Reserve Bank of India has reiterated that it never contacts the public via unsolicited phone calls or emails asking for money or any other type of personal information. The Reserve Bank does not maintain/give money/foreign currency or any other type of funds to individual or opens account for/in the name of individuals. The Reserve Bank has urged the public to remain alert and not to fall prey to frauds or scams perpetrated by individuals who impersonate to be employees of the Reserve Bank of India.\(^{189}\)

### 6.9 Conclusion

Therefore, it is observed that e-Banking means using the power of online networks, computer communications and digital interactive media to reach bank’s customers. Online banking does not replace traditional forms of banking anyway. Instead, it both adds to and subtract from today’s banking mix. It does add more interactivity, however, it does subtract costs. It facilitates customers as well as it removes dependence on paper work. Growing commercial concern about retention of customers is forcing the banks to implement more effective security environment. In order to provide strong shield to consumers from online frauds banks need strong security solutions to manage individual elements of their operations with secure and safe mechanism.

\(^{189}\) Alok Mishra and K.B. Asthana, July, 2012, pp. 82-100 at pp. 96-97.
It has been observed by the researcher that the *Bible of Cyber law* is the Information Technology Act, 2000 (2008). Whenever any illegal act occurs in cyberspace, all eyes look upon the Information Technology Act, 2000 (2008) for solution. After an in depth analysis of this Act, it is seen that most of the provisions are focused on penal provisions for disclosing of personal information either by body corporate or otherwise. No mandatory protection has been provided to consumers against offences like Phishing, Pharming, Cyber Money laundering, ATM Frauds and other financial frauds wherein innocent consumers are cheated and defrauded. Guidelines provided by RBI are just precautionary measures. In order to make e-Banking safe and reliable, it is very important to add penal provisions for day to day e-Banking frauds in the Information Technology Act, 2000 (2008).

Thus it is clear that in order to provide strong shield to consumers from Cyber money laundering, Phishing, Pharming, Credit Card Frauds, ATM Frauds and other online financial frauds, India needs specific stringent legislation. The Information Technology Act, 2000 (2008) has covered fraudulent financial activities indirectly. It is needed that these must be combined with a cohesive and comprehensive security provisions that enable them to have a clear protection against the threats to which they are exposed at any given point of time across the entire enterprise.\(^{190}\) The lack of a comprehensive legislation pertaining to privacy and data protection has been a matter of great concern in India. Even though the data protection laws are not specifically laid down in any statute as yet, however, with strict regulations and privacy norms recommended by the Reserve Bank of India, the Indian financial industry have begun the process of sensitizing the Government and people. In the process of sensitization the consumers must take a responsibility regarding the privacy as well as awareness in their day to day online transactions. In order to deal with online challenges it is very important to implement legal provisions effectively in the country.