The world of plastic money is indeed fascinating. In India, it is a growth industry and today command special focus of attention not only within the banking sector but also in the law. The plastic money was seen as infusing convenience, safety, speed and order in modern society. In short, it was a great subservient innovation until the monster within its reared head. This monster was the immense potential of the credit cards misuse and the perpetration of fraud (Mehta and Mehta, 2001). In the past few decades, banking institutions and law enforcement the world over have struggled to keep pace with various and innovative facets of plastic money fraud. In spite of the proliferation of plastic money in daily lives and despite the billions of dollars of fraud perpetrated using plastic money, it is one of least researched issue under law especially in India. This chapter covers the different types of frauds, their prevention and detection, fraud investigation, legal framework in India and U.S and the cross comparison of two countries.

4.1 Plastic Money Fraud

In the days when barter was the only way of obtaining goods, the fraudster would find it difficult to hide his neighbour’s bullock-cart. With the advent of money, he breathed a sigh of relief because money was anonymous and much less bulky than the bullock-cart. With the advent of credit cards, it was not anonymous like the paper money, card usage could be traced. For this fraudster had to adapt to the new situation, so he became a technically knowledgeable person and started using technology to his advantage, to commit fraud and monetarily benefits from it. Credit card fraud has been defined by ‘The Fraud Examiners Manual’ as “the misuse of credit card to make purchases without authorization or counterfeiting a credit card”. Bank credit card issuers lose about $ 1.5 to $ 2 billion every year because of fraud. The Visa and Master Card, the two largest credit card issuers lose most. Generally, the credit card fraud is
committed successfully on most of the occasions. Chances of being caught are small and the necessary legal procedure to book the culprit based on strong evidences is not available (Jagadeesh, 2005) Like other countries if the genuine credit card has come to India, the fraudulent credit card cannot be far behind. It is bound to cast its shadows far and near, throughout the sphere. And they will thicken every year. The banks are the most important institutions dealing with the credit cards frauds (Sharma, 2003). Credit card misuse is growing in popularity because it is easy, often anonymous and leaves no trace. Victims usually are ordinary citizens; most countries do not have specific legislation to address credit card fraud, according to Visa and Master Card Fraud Management. Credit card theft and misuse is committed every second across the world. There are no special segments or geographic areas. The universal acceptability of credit cards allows card numbers stolen in a country A to be counterfeited in country B, and used in country C. Card industry data shows that the United States accounts for more than half the total worldwide credit card fraud. But countries such as Taiwan, Hong Kong, Malaysia, Italy, Spain and Japan have a high card fraud rate. India is no exception to credit card fraud. The only consolation being that most of the frauds are small in value and can easily be checked (Prasad, 2002). It is feared that with the expansion of E-commerce, M-commerce and Internet facilities being available on a massive scale, the fraudulent fund freaking via credit cards will increase tremendously. The key man to call a halt to the credit card frauds is the man at sale terminal. However the person involved in the sale process do not scrutinize the cards well. Perhaps courtesy to the customer or collusion with the customer to make a quick buck are responsible. In one case a false visa card, carrying an image of a pig instead of a hologram of a dove, was used eleven times at the same sale terminal before the culprit could be caught (Sharma, 2003) The fraudster has many types of frauds up his sleeve. The fraud can be simple but ingenious, it can be technologically advanced, it can be of a type, which can be perpetrated by a single persons, or by a group of people. Every time the card issuers come up with a new security measure, the fraudster comes up with something to counter that security measure.
4.2 Types of Fraud

4.2.1 Application Fraud

The fraudster obtains all information of a person who would be eligible to get a card. He then applies to the issuer with that person’s information except for the address. The residential address of that person is substituted within fraudster’s temporary address. A variation of this fraud is that the fraudster obtains the card details of a genuine card-holder. He then calls up the issuer pretending to be the genuine card-holder to report his card as lost and to request the issuer to send the card at the new address. If the bank does not call up the card holder to confirm or verify the change in address, the fraudster will get a genuine card on which he can run up whopping bills.

4.2.2 Multiple Imprints

The fraudulent merchant may ask the card holder to sign on more than one chargeslip on some pretext such as print is not clear on the present chargeslip or the signature of the chargeslip does not tally with that on the signature panel of the card. The merchant then present these consecutive chargeslips to his acquirer with a gap of few weeks or even months. The acquirer makes payment because of the face to its signature imprints, etc. seems to be in order. The cardholder cannot deny the charges since he has himself signed on the chargeslip (Radha, 2004).

4.2.3 Sold Paper

When merchants submit consecutive chargeslips for the same cardholder at an interval of few weeks or even months, it would more often than not be a case of fraud. Also presenting the chargeslips after such a long period means an inordinate delay for the merchant in getting his money. In order to overcome this matter the merchant started ‘selling’ such fraudulent chargeslips to other merchants, who in turn submit the chargeslips to his acquirers. This is more difficult to trace. It is known as sold paper fraud since the paper, i.e. the chargeslip is sold to other merchants for a fixed price. The buyer merchant is then free to fill in any amount before submitting the chargeslips to his acquirer.

4.2.4 Altered credit card

The altered credit card is one which was originally genuine card manufactured and issued by proper authority. The original card is lost or stolen. It comes in possession
of the forger. He gives it a new entity by altering it suitably. It is re-embossed with a new name, an account number, a convenient expiry date, etc. The original signatures are changed sometimes but often the original signatures are allowed to remain and the defrauder practises to imitate them and acquires the skill to write the signatures on the sale draft and in other credit card transactions with passable resemblance (Sharma, 2003). It takes a long time to detect altered card forgery. Usually only when the account holder gets the statement showing the abnormal transactions. The forger gets the genuine account numbers fraudulently from his criminal contacts in banks, sale terminals of stores, etc. The altered card is not a normal card. In the altering process, heating is essential which disturbs the security features such as the identity number of the bank or the holographic insignia incorporated by the card issuers. It is rare that the altering process is near perfect. Unfortunately the person at the sale terminal does not bother to scrutinize. If he does, quite a few frauds via altered cards can be prevented. This fraud requires sophisticated technology which is as yet unavailable to Indian fraudster but is prevalent in the western countries and in Hong Kong and Indonesia.

4.2.5 Duplicate Card

The duplicate fraudulent credit cards are those where the defrauders have made sincere efforts to duplicate the original cards through photo-mechanical processes. They follow the footsteps of the original manufacturers of the genuine credit cards to produce as close a replica of the genuine card as possible, employing similar materials and similar processes of printings and embossing, besides magnetic encoding. In fact the work is being professionally done by some gangs (Frazer, 1985).

4.2.6 White Plastic

‘White Plastics’ are imitations of credit cards in general aspect. The forger does not make any serious effort for exact replications of dimensions, sizes or shapes of letters, graphics, etc. The counterfeit credit cards are poor imitations of the genuine cards and even a layman can distinguish one from the other, if the two are presented to him. The manufacture of the white plastics does not follow the pattern of the manufacture of the normal genuine cards. In white plastic fraud, it is not difficult to identify that of a fake card because the embossed figures of the card bin number are bound to be crooked and will not 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 are either not trained properly for it or they are so overworked that they don’t have the time to scrutinize each chargeslip as closely as it deserves to be.

4.2.7 Terminal Takeover Fraud

In this fraud, the fraudster does not collude with the merchant, instead he poses as the acquirer’s 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 also has the facility to store the credit card information obtained through the magstripe. After a few days, the fraudster returns the machine claiming that it has been repaired. He replaces his own machine with the original machine and disappears - alongwith all the confidential credit card data (Smith and Richard 1987)

4.2.8 Shave and Paste

Any number of alpha or numeric characters are sliced from the card other characters are attached to the card surfac utilizing fast drying epoxy-type glues. This is done to put an entirely new but valid account number as to change the name, so that the fraudster can use the card as if it is his own (Jagdeesh, 2005)

4.2.9 Identity Theft

One of the boom fraud type is identity theft. The simple fact, however, is that identity theft existed long before the internet. What the internet has done is to facilitate both the ease with which other people’s information can be obtained and then used. Identity theft is a blissfully concept; the fraudster illegally acquires and uses an innocent person’s personal details, credit as account information to obtain money, credit goods, services and anything else of value. All such spending or goods ultimately end up being recorded on the innocent victim’s credit record (Lilley, 2002). There have been numerous way of acquiring the required personal information to commit identity theft including stealing a wallet or a purse, going through trash and picking out financial statements or credit card slips or taking mails directly (Okula, 2004).

4.2.10 Lost/stolen card

A card holder can genuinely lose his card when he forgets to collect it from the ATM machine or the cashier after signing for the goods or loses his wallet with his card
in it and in many other ways. When a fraudster comes across such lost cards, either he himself uses the card or sells the card to a gang which specialises in credit card related crimes. This gang has recruits persons at various levels. Those who have to show their face in the shops by going there physically are called ‘runners’. These runners try out the cards at various establishments for the small amounts in order to ascertain whether the card has already been put on ‘hot list’. If the card is found to be ‘clean’, the card is immediately used for high value purchase-by forging the signature (Mehta and Mehta, 2001). There are instances of course, when the cardholder reports his card as lost and then himself goes on shopping. This can be done because once the cardholder reports his card as lost, his maximum liability is limited to Rs. 1000/-. When the cardholder is billed for the items purchased after the date of the card being reported as lost, the cardholder refuses to pay claiming that he had reported the card as lost and is therefore not liable to pay the charges. Stolen cards fall under two categories:

- Stolen in mail.
- Stolen from wallet, purse, house, car etc.

Stolen in Mail is also known as Not Received Issue (NRI). One of the simplest and yet the most effective way of obtaining genuine cards is by ‘intercepting’ the cards at the mailing stage. These cards are genuine and have a blank signature panel. The interceptor can sign on the panel any signature with which he is comfortable. The salesman never suspect him while he signs. Since the card is genuine, close scrutiny of it will not reveal any flaws such as defective signature panel or altered numbers etc. Hence it is treated as a genuine card.

4.2.11 Mail order telephone order (MoTo)

The highest percentage of frauds in credit cards in India happens in the mail order telephone order (Moto) type. These are the typical ‘cards not present’ type of transactions where the card owner furnishes the card details over phone like his name, date of birth, card number, card expiry date and his address for verification (Prasad, 2002). The fraudster act as a representative over the phone, and get the full details. Many cardholders fall victim to this tactics. This card number is used to purchase a lot of material through catalogues and mail orders. The fraudsters would give an address not occupied by him, and then later collects the material from the parcel service offices.
4.2.12 Merchant Collusion

Merchant Collusion is said to occur when the merchant colludes with the fraudster by providing information regarding genuine credit card. The merchant can allow fraudster 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 a 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 issuers at a later date. The information can be used to manufacture counterfeit cards or to obtain genuine cards by reporting the cards as lost or to defraud by mail order. There are instances where the customer himself colludes with the merchant to defraud the issuer. He uses the card at the merchant’s shop for a single transaction but allows multiple imprints of his card to be taken. The merchant submits these imprints with forged signatures and obtains his payment from his acquirer. At the end of the cardholder’s billing cycle, when he is billed for payment, he claim fraudulent transactions and refuses to pay up. The merchant has already been paid and the card – holder refuses to pay so it is the issuer who has to bear the fraud loss. It is difficult to prove such collusion until and unless the same card-holder keeps appearing in many such cases of fraud (Mehta and Mehta 2001)

4.2.13 ROC Pumping

A merchant, with fraudulent intention, takes more than one imprint of the cardholder’s card on the imprinter. Frequently, the imprints are not taken in front of the cardholder, as in case of restaurant where the card is taken by a waiter to the cashier, or at hotel check out counter, where the cardholder is unable to watch the procedure clearly. Once the merchant has the imprints of the charge slips, the forges the cardholder’s signature from the original charge slips and present the chargeslips to the acquirer after a gap of a few weeks. The acquire pays up the amount if the forgery is done well. But the cardholder is likely to dispute the charges and the signature and therefore refuse to make payment. In this case, it is the acquirer and / or the issuer who has to suffer. In this type of fraud, the merchant requires Original Charge Slips to make or pump more charge slips. The fraud is therefore termed as ROC pumping fraud (Joseph, 1996).
4.2.14 Skimming

As technology develops so do the types of frauds. The latest fraud happening abroad is skimming. In simple terms catching the CVV (Customer verification value) data. CVV is an algorithm (a code) which is very difficult to break through. The fraudster therefore does not bother to do so. He simply colludes with a merchant or merchants. He then provides the merchant with a terminal similar to the one provided to the merchant by the bank. This type of scheme usually occurs in businesses where the patron’s credit card is taken out of sight while the transaction is processed (Barker, 2008).

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 bank’s terminal only processes the data but does not have a recording facility. The merchant swipes the card twice; once 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 now has genuine card information along with the CVV for each card. This is a goldmine for making counterfeit cards as far as fraudsters is concerned.

4.2.15 Phishing

This type of cyber crime is growing rapidly. The fraudsters (fishermen) send out a large amount of emails (the “bait”) directing the victims to their phony web sites. The e-mails appears to be from organization like banks, e-Bay, AoL and Pay Pal asking the victim to enter their personal information to clear up a “Problem” (Barker, 2008). It relies on the ability of the perpetrator to fool a victim and that usually involve web spoofing. Spoofing is the imitation or mimicking of a legitimate website, e-mail or entity communication in order to trick the recipient into believing the communication or website is trust worthy. Thus phishing involves the use of seemingly legitimate communications that is spoofed to deceive bank customers into disclosing sensitive information such as ATM PIN, Number, credit card data, passwords or financial personal identification numbers. Most often the purpose of Phishing is to gain sufficient information to perpetrate. Customers should be aware of limited web resources and they
should not provide their confidential information regarding their accounts, card number, PIN’s etc to unknown people (Bhasin, 2007).

4.2.16 Lebanese Loop Fraud

This is a device used to extract the card information. Here a magnetic tape along with a hook blocks is attached inside the card-reader. When the customer inserts the card the hook blocks his card inside the ATM machine. The scamster suggests the customer to enter the PIN number so as to help him out of the situation. Unable to get the card, the customer leaves the ATM location thinking that the machine has malfunctioned and retained the card. (Krishna 2007). The scamster then removes the magnetic strip and the card. Thus the PIN information and the card are used together to defraud and the customers. The preventive measure for this fraud is to report to the bank through an ATM hotline number given by different banks to stop any withdrawals from the account.

4.2.17 Shoulder Surfing

This is another very simple technique where the fraudster employs to get himself into possession of an innocent customer’s confidential financial information. The fraudster stands behind the genuine customer at ATM centre and pretends that he is on queue to get cash withdrawal from ATM. While the genuine customer performs the banking function, he steals the PIN numbers to use it in fraud after the customer has gone. These cases are becoming common as ATM machine are not monitored an account of how many customers entering the ATM machine room. Banks should increase security like closed circuit camera which is monitored 24 x 7, to mitigate this kind of menace.

4.3 Prevention and Detection

In the retail environment, there is a need for verification of the card holder’s identity at the point of sale. Current techniques, such as the visual inspection of signatures or the use of holograms offer some protection against plastic card fraud. Unfortunately, knowledge can be stolen or replicated and signature can be forged. While photographs and PINs discourage forgery, they fail to link the card uniquely with its authorized user. Many banks use sophisticated “artificial intelligence” of neural
networks, statistical models and other predictive techniques to find unusual spending patterns and thereby preempt fraudulent transactions. “Smart cards” use embedded computer chips instead of magnetic strips to secure information. France has used this technology successfully but the option has not succeeded globally yet. While biometric technologies have the potential to reduce plastic card fraud. Using biological traits such as retinal or iris scanning, finger prints, or face recognition – is touted as the future of the payments industry. But there are several problems which must be addresses before they can be used in retail environments. One of prime concern is the recognition performance of the biometric technology. Sometimes even legitimate user may object to providing prints. Ideally, the technique used must cope with the requirements that it must reject all impostors while at the same time not rejecting valid customers. Most biometric technologies are still in the early stages of the development life cycle. To improve reliability and reduce costs in the long term, it is difficult to predict which of the biometric technologies will become dominant. Merchant and customers ignorance about card security features and guidelines frustrate card issuers.

At institutional level all card issuers like VISA, MASTER and AMEX must have their own unique features to prevent the fraud or misuse of the credit cards. Computer edits are inbuilt in some cards, so that the user is fixed a limit in terms of number of times the card is used or the amount of money spent in a particular month. Credit card fraud could be reduced substantially by giving holders a secret personal identification number (PIN) that they have to punch in before every transaction. Cards with PINs are available in many countries, but switching to such a system a complicated and expensive.

At merchant level staff members handling cards should be trained on card security features like hotlisted cards and suspicious behaviour of cardholders. Merchant establishments should maintain card data securely in computer systems and records. They should keep a close tab on employees handling credit cards. They should be subject to the same level of safeguards as if they were handling money. For security
precautions such as store cameras and staff identification should adequately maintained
(Moller, 1981).

At cardholder level, cardholder should always keep the card in a safe place and never lend to anyone. If the card is lost, stolen, retained by ATM or there has been an unauthorized transaction, cardholder should notify their financial institution immediately. For this, cardholder should always examine the charges on credit card statement before paying them. As a precautionary measure, the cardholder should not give credit card number, personal information, bank account number over the phone or to any person or company having only a web site or mailbox drop. It is advisable for the cardholder not to carry extra credit card or other important identity documents except when needed. Some preventive tips should be followed by the cardholder like don’t allow sales clerk to copy credit card numbers on checks for additional information or to use credit card as identification, use a credit card instead of a debit card; debit card don’t have maximum liability for fraudulent use, sign credit cards in permanent ink as soon as they are obtained, don’t let waiters, sales clerks or gas station attendants disappear from view with credit or debit card; to avoid “skimming”. Crooks can copy the information from card’s magnetic strip. By Installing firewalls and virus-detection software on home computers can discourage hackers. If cardholder become a victim, they should immediately report the crime. Filing a report with local police and keeping a copy with themselves will make it easier to prove their case to creditors and merchants and may help them to build lawsuit if cardholder have to sue to recover losses. As long as credit cards in existence, the related credit card frauds are bound to happen. Many fall prey to the fraud. The issuer look for newer methods to prevent such frauds. It is in their own interest that the cardholders should keep their cards safely and use the cards wisely to protect themselves from frauds.

4.4 Fraud Investigation

Once the fraud is detected or suspected, the stage is set for the investigation of the same. Investigation refers to the search, inquiry or formal examination or study
conducted in order to ascertain the truth of any incidence, circumstance, event, document, person or state of affairs. (Mehta and Mehta, 2001).

Investigation in the case of credit card fraud is done at two levels:-

**External investigation and Internal investigation**

4.4.1 **External Investigation**

External investigation refers to the investigation of the credit card fraud by an outside investigation agency such as the police or the private investigator. The card products industry in particular and the banking industry in general works very closely with the local, national and at time even international police. Within the local police itself, the banking industry is in constant touch with the economic offence unit and which unit is a specialized team of police investigators having specialized knowledge and data base useful in ‘cracking’ frauds. When a fraud is suspected to have taken place involving more than one state then federal or union police (such as FBI or CBI) may be contacted. Frauds, which exhibit the handiwork of international gangs or where a card stolen from one country and is sought to be misused in another, involve the working in tandem of the police forces of two or more countries and is mostly coordinated by INTERPOL (White 1991). Within a particulars police department there are other units which render great service in solving credit card frauds. Some such units are:

- The forgery and Anti-Counterfeiting Department
- Fingerprinting
- Handwriting Experts
- Modus operandi unit
- Criminal investigation Department (CID)

i) **The forgery and Anti-counterfeiting Department**

These sleuths called the ‘Paper tigers’ are experts in investigating forgeries. The investigating detective of the forgery and anti-counterfeiting unit work closely with the *modus operandi* and handwriting/signature experts. They also have a network of informants who supply them vital clues about who (or which gang) has pulled-off the fraud. Over a period of time these ‘paper tiger’ build a strong data-base of information on various forgers and the type of forgeries they normally commit.
ii) **Fingerprinting**

Contrary to common perception, paper (especially certain kinds of paper) are perfectly capable of retaining fingerprints. Sales receipts, charge-slips, invoices and other documentation with fingerprints provide an important source of information to the police to track-down the fraudster.

iii) **Handwriting Experts**

The credit-card fraud is essentially a ‘Paper Fraud’ and normally wherein the fraudster has to sign or write at some place. This piece of evidence which again may include charge slips, invoices, delivery challans and other documentation such as card application forms, cheques signed by fraudster, etc. can prove to be the ace, not only to track down the fraudster but also to convict him.

iv) **Modus operandi unit**

The _modus operandi_ wings are specialists in and maintain a data-base not only to various criminals but also their method of operation (_modus operandi_). Thus when a particular kind of fraud takes place, the modus operandi sleuths can try and match the type of fraud or crime to a particular ‘known’ fraudster or criminal. Further, most credit card frauds take place in a manner wherein the fraudster has been seen by some human witness such as bank staff, security guards etc. and therefore identifying him gives the police a major breakthrough. _Modus operandi_ wing maintain both computerized and photographic records of such known criminals as the witness may then be able to view the same and identify

v) **Criminal Investigation Department**

The Criminal Investigation Department or what is popularly called the C.I.D are experts in criminal investigation techniques. They unlike the forgery unit are the ‘generalists’ of criminal investigation. The C.I.D., at times, in conjunction with the economic offences unit undertake undercover ‘sting’ operations, especially to combat credit card frauds which involves merchant collusion. A sting operation is an undercover police operation in which police pose as criminals to trap law violators and fraudsters. It has to be understood that sting type undercover operations are controversial since they involve a police officer becoming involved in illegal activities and encouraging offenders to break the law. The bottom line is that sting operations
have a permanent place in the Criminal Investigation Department’s repertoire of law enforcement and credit card fraud investigation (Mehta and Mehta, 2001). Stings are employed in the investigation of card frauds where merchant collusion is suspected. Normally, such suspension is aroused by the fact that a particulars merchant or group of merchants have a high rate of fraud incidence within their shops/establishments as compared to other merchant establishments and as compared to their sales volumes.

4.4.2 Internal Investigation

Internal investigation refers to the investigation of the credit card fraud by the personnel of the credit card issuing bank. Internal investigation has two aspects; firstly, internal investigation may be actually investigate the fraud perpetrated in the said case. Secondly, internal investigation could be an investigation of such a nature which mitigates the possibility of the said fraud continuing. Needless to say, the two prime reasons for conducting internal investigation are to reduce the quantum of the fraud and to attempt to pinpoint and apprehend the perpetrator (Khumalo, 1992). There are some below important aspects as internal investigation.

i) Specialist Fraud Investigation Team (Internal)

The fraud investigation Team consists of ‘Specialist’. The team members have specialized knowledge, which they have acquired due to longevity in the said function. Fraud Investigation Teams are aware of, understand and can analyze typical modus operandi of the fraudsters. They have with them ready made ‘best practice’ templates. Thus the fraud investigation team also builds over a period of time a good rapport and understanding of the workings of the police department especially the Economic Crime Unit and the Criminal Investigation Department.

ii) Networking with competitors

The Fraud Investigation Team works continuously with competitors to understand repetitive forms of fraud and fraud perpetrated by the same person and/or gangs. Almost all major internal investigation begins with calls to the other credit card issuers to try to get leads of the case of question.
iii) **Internal intelligence Gathering and statistics**

Internal Reports, Statistics and Intelligence gathering is base on which edifice of the Fraud investigation Team is build upon. Important aspects of this issue include early warning systems, new fraud trends, proactive fraud control method, proper methodical and perfect credit card documentation card holder’s billing, original card application and charge-slips.

iv) **Internal ‘Red – flagging and caution Signals**

A vigilant internal investigation team relies largely upon computer controlled danger signals or what are called ‘red-flags” (Smith and Richard, 1987). The Computer are programmed in such a way to give a monthly report on various merchant establishments where frauds have taken place. If a particular merchant establishment is repeatedly shown as a place where frauds are taking place, then Fraud Investigation Team immediately investigates that particulars merchant establishment thoroughly.

Similarly, the computer are geared and programmed to immediately draw the attention of the Fraud Investigation Team if abnormal credit card transactions/activities are noticed. For example, if a particular cardholder habitually spends between Rs. 2000 to Rs. 5000 a month and suddenly in a particular month his spending is 10 times of that amount, then the computer draw the attention of the bank to this fact which may require immediate investigation.

v) **Data on Direct Sales Agents (DSAs)**

DSAs procures business for the card issuer. In short, it is outsourcing of marketing/sales. A proper investigation control of the DSAs can bring to light the rate of the fraud of clients to whom cards were sold by a particulars DSA. Thus, if the rate of fraud and/or delinquency is much more of clients who have been sold the card by a particular DSA then this fact needs investigation and rectification (White, 1991).

### 4.5 Legal and Regulatory Framework

Plastic money is established as feature of the commercial scenario. But surprisingly, there is very little discussion of their legal aspect. The regulation of plastic money business in India is diffused and needs to be streamlined. Whereas in developed countries like United States, the law on plastic money business is comprehensive and
straightforward, its Indian version requires a structural change. Even though the apex bank i.e. RBI has formulated a few guidelines on the international credit cards. Debit cards and Smart cards, an efficient regulation on credit card business is still a long way to go. An attempt has been made to cross compare the credit card regulation mechanism in United States and India from the viewpoint of the consumers.

4.5.1 Indian Version

Credit industry’s legislative premises in India card industry’s legislative premises in India are primarily confined to the “Common Consumer Law i.e. the Consumer Protection Act, 1986 and the General criminal Law i.e. The Indian Penal Code, 1860”. In Addition, the related legislations like Banking Regulation Act, 1949, Income Tax Act, 1961; RBI Guidelines etc. partially regulate the card business in India.

i) Indian Contract Act 1872

The “Credit” is given to the customer by the supplier on the basis of card. In a credit card transaction, three parties are involved, namely, the issuer, the customer or card holder and the supplier. The card holder, on the strength of the card, purchases goods or service from the supplier. The supplier recovers the price of the goods or services from the issuer. A credit card scheme is worked on the basis of a number of contracts as (a) there is a contract between the issuer of the card and the holder of the card. (b) The Second contract is between the issuer of the card and the supplier (c) the two contracts made above are prior to the individual transaction of sale that comes to be entered into between the customer and the supplier. This transaction of sale is subject to a special feature not found in cash sales. The purchaser (cardholder) is not required to pay cash to the supplier for the goods or services supplied to the cardholders. If the supplier insists on cash payment and refuses to give credit, the customer has no legal remedy against the supplier, because there is no privity between the two. The supplier refuses to give credit, the customer’s only remedy is to sue the issuer of the card for breach of contract. In an ordinary credit sale (not involving the use of a credit card) the seller has the right to recover from the purchaser the price, if not paid by the expiry of the period for which credit is given. But, in the case of a supply on the strength of credit card, once the supplier accepts the voucher signed by the card-holder, the supplier’s
rights against the customer come to an end. The card holders obligations to the supplier are absolutely discharged by the suppliers acceptance of the vouchers signed by the customer. The reason is that the supplier knows that on signing the voucher the customer renders himself liable to pay to the issuer of the card the price of goods obtained on credit from the various dealers who have joined the scheme. Further, there is already an agreement between the issuer and the supplier that the supplier shall be reimbursed for the credit given by him to various card holders. The supplier has a remedy against the issuer of the card and need not have a double remedy against the customer. The confusion is created by use of the word “Credit Card”. The transaction is not merely a sale on credit. It is really a complex one, involving:

i) Sale on “Credit”, but only in a limited manner.

ii) Reimbursement to the supplier by the issuer;

iii) Debit by the issues against the customer. In an ordinary sale on credit there are only two parties – the purchases and the supplier. In a credit card sale, there are three parties – the customer, the supplier, and the issuer of the credit card. Besides this in an ordinary sale on credit, the supplier gives credit on the basis of the financial credibility of the purchaser in contrast. In the case of a transaction in which a credit card is accepted by the supplier, the supplier gives credit on the strength of the financial credibility of the bank or other agency that has issued the card (Bakshi, 1993). A word may be said about the transaction effected between the supplier and the credit card holder. It shows that these conditions attracts even to a sale on credit card. The only difference is that the customer (cardholder) does not pay the price in cash, but pay it in the form of the promise made by the card-issuing agency to reimburse the supplier on the strength of vouchers signed by the cardholder.

ii) **Indian Penal Code 1860**

The provision of the Criminal Law contained in IPC are applicable to the credit card business. The credit card arrangement is a civil law transaction and is fundamentally not the concern of the criminal law except in extreme cases. Section 378 deals with theft under the Indian criminal justices of the Indian Penal Code, 1860. The intention of taker will determine whether the taking or moving of credit card is theft. Under the law where there is no intention to take the card dishonestly there is no theft.
The cardholder also comes under the provision of theft, if it completes the application form for credit card and gives false information, address, references and having no intention to repay the money an account. Section 379 of the Indian Penal code deals with imprisonment (simple or rigorous) for three years or with fine or with both for the theft of credit card. The law stipulates for a much harsher punishment which may extend to 7 years, if the theft is by the clerk, having the card in possession of his master. The issuing bank can charge the credit card holder under Sec 415 for cheating if the issuing bank shows that cardholder had no intention to repay at the time he applied for the card. The punishment of cheating is stipulated by Section 417 and entails an imprisonment (simple or rigorous) upto a year or with fine or with both. If the cardholder had applied in a false or fictitious name then he may be also booked under section 416 (cheating by Personation). This offence is committed when the individual personated is real or imaginary. Cheating by Personation attracts imprisonment (simple or rigorous) which may extend to three years or with fine or both under Sec 419. Sec 420 could be pressed if the misuse of the credit card is such that the person cheats another and thereby dishonestly induces the person to deliver any property. This Section attract an imprisonment of seven years and fine. Credit card fraud is a big business and one of the latest ‘fads’ amongst organized crime syndicates. Credit card fraud is operated on large scale, the card may pass two, three or more parties (or gangs) before it is actually misused. The person who actually steals the card can be booked for theft under section 378 and the person who actually gets the delivery of the property by misusing the card may be charged with cheating under section 415. Cheating by Personating (Section 416), or cheating and dishonestly inducing delivery of property (Section 420). However the intermediaries (for example, the person who receives a stolen card and sells it to another) charged under Section 411, which deals with dishonestly receiving stolen property. If the prosecutor will prove under section 412 that credit card was stolen in the commission of a dacoity, then the intermediary (person receiving the stolen card) faces a maximum imprisonment for life or with rigorous imprisonment for a term which may extend upto ten years. But if the card holder is waylaid by a gang of five (or more) persons and his wallet containing the card is taken by them at knife point then all five shall be guilty of ‘dacoity’ under Section 391.
if the cardholder is waylaid by a goon and his wallet is taken away on gun point or knife point then the ‘theft’ of the card is robbery under section 390 of the Indian Penal code. With the advent of organised crime in credit card fraud, the techniques used by the organized syndicates have been refined and restructured to actually include counterfeiting credit cards. Section 463, 465, 475 deals with the cases of counterfeiting cards and carries a heavy punishment of imprisonment (simple or rigorous) upto seven years and five. Sometime issuing banks receives false, fabricated and forged applications for the issuance of credit card, the normal reaction after examining the fabricated application to reject and applicant informed, as end of matter. The banker is a businessman and until he himself is hurt, he will not rise form his slumber. So sharing of data may help to a very limited extent in preventing the application fraud. Unless and until the various issuing banks come together and form a united front to fight the ever-growing threat of application fraud. A reduction in application frauds will not come by unless the message sent to application fraudsters is that they shall be prosecuted for even attempt to procure a credit card by deception.

iii) The Negotiable Instruments’ Act, 1881:

The government by its famous notification inserted by way of a new chapter XVII to the negotiable instruments Act, 1881 published in the Gazette of India Extraordinary, brought in a stipulation that a person issuing a cheque would be committed a criminal offence if the cheque is dishonored for insufficiency of funds. Credit cards are not negotiable instruments but this notification has strengthened the hands of the credit card issuer (bank). The Act has given them a device by which they could convert a civil matter into a criminal one. This conversion can take place only if the card issuer (bank) can convince the credit card payment defaulter to issue to the bank a cheque. And if the cheque is dishonored (for insufficiency of funds) there is scope to convert the mattes from ‘civil’ to a ‘criminal’. Section 138, 139, 140 of the Act deals with the dishonour of cheques. Section 138 of the Negotiable Instruments Act does not contain the procedure of filing the complaint in the court. While filing the complaint the bank must make specific averments with regards to monetary transactions for which the cheque was issued by the card-holder. Copies of the documents like credit card contract and chargeslip signed by cardholder, any correspondence sent to or
received from the cardholder regarding the payment, original dishonoured cheque, original returning memo issued by bank, notice served upon the cardholder as required under Sec 138, must be annexed for the perusal of the court. If the cardholder is found guilty of transgressing section 138, the court can punish him with imprisonment for a term up to one year or with a fine which may extend to twice the amount of the cheque or with both.

iv) The Consumer Protection Act, 1986

The consumer protection Act, 1986 provides an apex platform for the redressal of grievances of credit card holders. As per the definition of under the credit card holder is a consumer according to the definition of “consumer” under the Act, since he hires or avails of services for a consideration. Accordingly, the credit card issuers are legally responsible for any deficiency in services or unfair trade practices. Section 2 (g), 2 (O) and 2 (r) of the Act define the terms “Deficiency”, “service” and “unfair trade practice” respectively. The Act envisages three tier quasi-judicial machinery at the National, State and District levels. National Consumer Disputes Redressal Commission known as “National Commission”, State Consumer Disputes Redressal Commission known as “state Commission” and Consumer Disputes Redressal Forums-known as “District Forum”. A Complaint can be filed under Section 12 of the Act by a consumer, any voluntary consumer organisation registered under the Societies Registration Act, 1860 or under the Companies Act, 1956 or under any other law for the time being in force, the Central Government, the State Government or Union Territory Administration or one or more consumers on behalf of numerous consumers who are having the same interest (class action complaints). Under the Act, a complaint means any allegation in writing made by a complaint which inter alia includes unfair and restrictive trade practices and deficiency in services.

A complaint should contain information about the name, description and the address of the complainant, name, description and address of the opposite party or parties, the facts relating to complaint and when and where it arose, documents, if any, in support of the allegations contained in the complaint, the relief, which the complainant is seeking, the complainant or his authorized agent should sign the complaint. The complaint is to be filed within two years from the date on which cause
of action has arisen. Section 11, 17 and 21 provides for segmented redressal machinery for filing of complaints based on the value of the claim lodged:

- Upto Rs 500,000- District Forum
- More than Rs 500,000 and less than Rs 20,00,000. State Commission.
- Exceeds Rs 20,00,000- National Commission

Generally, the credit cardholder falls in the first category. The procedure for filing complaints and seeking redressal are simple enough. There is no fee for filing a complaint before the District Forum, the State Commission, or the National Commission. The complainant or his authorized agent can present the complaint in person or it can be sent by post to the appropriate forum/commission. Aggrieved cardholder can see the relief under section 14 of the Act depending on the nature of relief sought by the consumer and the facts of case. The aggrieved cardholder can appeal against the order of district forum/state commission/national commission within a period of 30 days respectively. Procedure for filing the appeal is same as that of complaint, except the application should be accompanied by the order of the District Forum/State Commission as the case may be specified for filing the appeal should be specified for filing the appeal should be specified. Based on above, it appears **prima facie** lucrative for the consumer to seek remedy under the 3-tier machinery under the Act. However, the story is altogether different. Following issues are important to be considered in this regard.

- In their card application forms, the issuers specifically indicate the jurisdiction in case of dispute, which is major problem to the redressal process. A Citibank credit card holder in Delhi is entitled to seek relief only in the consumer forums/courts of Chennai.
- The consumer courts are presently flooded with a pile of pending cases, which renders logically impossible for a credit card holder to file a complaint.
- The credit card regulations are not circulated/shown to the cardholders at the time of issue. During a study, it was noticed that to none out of 50 cases of prospective cardholder the regulations were shown. Interestingly every sales man replied that “*if want to known about the regulations, you can visit the regional office*”. To add, the salesman themselves were not aware. Of course, most of the prospective
cardholders were also not interested. However, a gist of some conditions required at operational level was advertised only with the sole objective of business.

v) **Income Tax Act 1961**

The Income Tax Act 1961 compulsorily provides for filing of return by the credit cards holders. Section 139(1) of the Act states, inter alia that a person residing in a specified area (notifies by the Central Board of Direct Taxes) shall submit his return of income in Form 2C if he is a holder of a credit card (not being an add on card) issued by on bank or an institution. The above provisions do not apply to non residents and other persons as may be notified by the government. Non filing of return under proviso to Section 139(1) attracts penalties in the form of interest, summons, inquiries and other costs. Due to this reason it is found that some people are reluctant to buy credit cards inspite of the fact that credit card issuers are repeatedly convincing people that their identity shall be kept confidential. Section 17(2) of the Act provides that in valuation of perquisites the amount of expenses including membership fees and annual fees incurred by the employee or any member of his household, which is charged to a credit card, provided by the employer or otherwise paid for or reimbursed by the employer shall be taken to be the value of perquisite chargeable to tax. However there shall be no value of such benefit where the expenses are incurred wholly or exclusively for official purposes and certain conditions are fulfilled.

vi) **The Information Technology Act, 2000**

The Information Technology Act, 2000 has described various offences and prescribed punishment for the commission of such offences. Though the Act, 2000 has not defined certain contraventions and offenses, they can be interpreted in relation to the nature of offence under the Indian Penal code, 1860. The nature of offence of ATM frauds is dealt under section 66 of the IT Act 2000, which explains about hacking. This crime is fast growing in India and other emerging markets where computer knowledge is in possession of the few. The punishment for hacking in India is imprisonment upto three years, or with fine, which may be extended to two lakh rupees, or with both. This Act faces dilemmatic situation is some international cases where the jurisdiction is in a different country. Also, the penalty prescribed may be less when compared to the extent
of loss. Ideally the damages must be over and above the damages caused. For instance a person causes a loss of 100 crore but punished by being imprisoned for three years with fine of two lakh rupees in not ideally. Under the proposed amendments, banks can be held liable for being negligent in handling the sensitive personal data. After Section 43, which explains about penalty for damage to computer, computer system etc of the principal Act, 2000, a new Section 43A has been inserted which deals with compensation for failure to protect the data. The Section states that the bank or corporation shall be liable to pay damage by way of compensation not exceeding five crore rupees to the person so affected. Under section 70A, the Indian Computer Emergency Response Team (CERT-In) shall serve as anodal agency in respect of the critical information infrastructure for coordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report. Under section 79 (3), an intermediary who conspired or abetted in the commission of unlawful act as also made liable.

vii) The Foreign Exchange Management Act, 1999

Section 2 (c) of the Act defines an Authorized Person. RBI may authorise, revoke or give directions to Authorized Persons who deal with the foreign exchange under Section 10 of the Act. Card issuers are covered by the said provisions of the Act.

viii) Payment and Settlement system Act, 2007

The Reserve Bank, as the central Bank of the country has played a catalytic role. Over the years, in creating an institutional framework for development of safe, secure, sound and efficient payment system in the country. A major milestone was achieved when the Payment and Settlement System Act, 2007 was enacted empowering the Reserve Bank to regulate and supervise the payment and settlement systems, lay down polices to this effect and provide a legal basis for multilateral netting and settlement finality Accordingly, the Reserve Bank framed and notified the “Board for Regulation and Supervision of Payment and Settlement systems Regulation, 2008” and “Payment and Settlement System Regulation, 2008” for operationalisation of the Payment and Settlement Systems Act. (RBI annual report 2008-09)
xi) Reserve bank of India framework

a) RBI Norms for Issue of Debit and Smart Cards

The RBI has put a host of restrictions on the issue of debit cards and smart cards by banks. In its guidelines on the issue of debit / smart cards announced on 16th November 1999, the RBI has barred banks from tying up with non bank entities and the use of such cards to withdraw cash / make deposits from the point of sales. It has also imposed existing reserve requirements on smart card balances. RBI has permitted banks to introduce smart / debit cards with the approval of their board without any prior approval of the RBI. The smart / debit card operations have to be reviewed at half yearly intervals with fortnightly reports on operations sent to the RBI’s monetary policy department. The Scope of Smart / Debit card has also been extended to include electronic payment involving the use of card, in particulars at the point of sales and such other places where a terminal / device for the use/access of card is placed. The definition includes automated teller machine cards under its scope. According to the guidelines, a function of a card, which contains monetary transactions is included in definition of smart cards. Therefore prepaid cellular phone cards with stored value are also included. The RBI has also barred merchant establishment from releasing cash to cardholders. In terms of the regulation, “no cash transactions can be offered at the point of sale, with the smart/debit cards under any facility, without prior authorization of RBI under Section 23 of the Banking Regulations Act, 1949.” The RBI has advised banks to look at the financial standing of customers before issuing smart/debit cards to customers having good, financial standing and who have maintained the accounts satisfactorily for at least six months. However, banks can issue on-line debit cards to select customers with good financial standing even if they have maintained to accounts with the banks for less than six months. Banks can also extend the smart / debit card facility to those having saving bank account/ current account/ fixed deposit account with built-in liquidity features maintained by individuals, corporate bodies and firms. No smart/debit card facility can be extended to cash credit / loan account holders. However, issue on-line debit cards against personal loan account, where operations...
through cheques are permitted. In case of debit cards or on line, the payment of interest should be in accordance with the interest rate directives issued to banks from time to time under the Banking Regulations Act, 1949. Also, the onus of security of the smart card is on the issuer and that losses incurred by any party on account of breach of security or failure of the security mechanism shall be borne by the bank. The RBI has also barred banks from issuing unsolicited smart/debit cards unless it replaces an existing card. The guidelines provide for the following security aspects which include ensuring full security of the smart card, restrictions on dispatch of unsolicited cards other than replacement of card to the existing cardholders, maintenance of records, provision of information to the consumers, limits on losses borne by customers in case of card frauds means for notification of card losses, action to be taken by the bank, etc. (www.rbi.org.in/circulars)

b) Prudential Reporting Norms for Banks

The RBI has promulgated new asset classification norms and capital adequacy regulations for banks applicable from the financial year 1998-99. Under the norms, banks have to disclose the amount outstanding in their credit card operations in their balance sheets under a separate head. (www.banknetinida.com)

c) Guidelines on Domestic Credit Cards

Banks and their subsidiaries in India may freely issue credit cards valid in India, Nepal and Bhutan to non-residents of Indian nationality/origin. Claims arising from use of such cards may be settled in rupees by debit to accounts maintained with authorized dealers in India by the account holder or by inward remittance from abroad. However, no remittance from India will be allowed in settlement of bills in if these cards are being used in other countries. (www.rbi.org.in/guidelines).

d) Entry Barriers for Credit Card Issuers

RBI has placed restrictions to limit the players in the business by laying down a Rs. 100-crore net worth criterion for new ventures.
The RBI move has been promoted by the rising incidence of defaults by credit card holders, and is designed to keep out banks, which are not strong enough to cope with the problems posed by truant customers.

Also banks which intend to issue credit/debit cards either independently, or in tie-up with others, will have to meet the minimum net worth criterion before they seek board clearance. Net worth is computed by subtracting total liabilities from assets. (www.bengalonthnet.com/news/December2000)

e) **Guidelines for credit card operations**

The scope of the proposed guidelines spans a whole gamut of credit card operations touching upon card issuance, interest assessments, billing, customer rights, information privacy and confidentiality debt collection practices, outsourcing activities and redressal of customer grievances. The creditable and customer friendly features of the proposal that the terms and conditions of the credit agreement should be disclosed in clear and simple language in all important communications to the customers. The interest calculation must be explained with illustrations in each billing statement dispatched to customers. The credit card companies should send their billing statements without delay and customers must be given at least 10 days for settling their bills before interest assessments can kick in. Personal information of customers should be held confidential and cannot be shared with third parties. Debt collectors should not resort to verbal or physical intimidation or harassment of cardholders, their friends and family. The credit card companies are liable for the action of third parties hired by them for sales or collections. Customer complaints should be resolved within 60 days. The RBI guidelines though covering a lot of ground, however, are not free from their baggage of controversies, limitations and omissions. The credit card companies are now authorized to issue the plastic to only those consumers with independent financial means. The card issuers are explicitly forbidden from signing up students into their portfolio. Expectedly, this rule has been greeted with consternation by the industry. It will elicit a similar disapproval from the student population and is also bound to take some fun out of their ephemeral and insouciant school life. There is a provision to prohibit the
issuance of credit cards to minors, criminals and anti-nationals. The right of approving otherwise bonafide customers should remain with the risk taker and not the regulator. The number of credit cards and total spending limit to approve or avail of, are decisions best left to card issuers and their customers.

f) Guidelines on Dollar Card
The RBI has issued the following guidelines on Dollar Card:

- For personal travel, the credit card holder can spend up to a maximum of $3,000 per annum.

- For Business travel, there are two categories- Any executive of a corporate can spend a maximum of up to $350 per day and directors and senior managers can spend up to $500 per day.

- A cardholder can avail of both entitlements based on need or business travel quota (BTQ) for personal travel.

- The card issuing bank/organisation should obtain from the applicant in the application an undertaking that the issue of strictly in accordance with the exchange control regulations and in the event of any failure on the part of the later, the applicant and/or its officials would, besides being liable for action under FEMA, 1999, be debarred from ICC facility either at instance of the RBI or card issuing bank/organisation in India.

- The applicant is also required to provide an undertaking that the actual utilisation of foreign exchange and the settlement of foreign accounts will only be through the designated branch of the authorised dealer.

- On receipt of application from the cardholder or the concerned parties for availing the ICC facility in addition to exchange in the form of currency notes and/or traveller’s cheque, the designated branch of the authorised dealer should advise in writing the foreign exchange entitlement of the cardholder which must not exceed the limits set by RBI for the release of foreign exchange for travel abroad for various purposes under the authority delegated or permission granted by the RBI. Payment for ICC is made through dollar draft through an authorised dealer or by direct debit to an Exchange Earnings Foreign Currency (EEFC) account. Delay in payment, if any, needs to be
referred to RBI explaining the circumstances, which have led to the demand for the late payment fee. (www.rbi.org.in/publication)

g) **Guidelines on International Credit Cards (ICCs)**

RBI guidelines on ICCs provide that Banks or their subsidiaries in India do not require permission from RBI from exchange control angle for issue of ICCs to residents. The credit card issuing banks or subsidiaries may remit to the overseas organisation with whom they have tie-up arrangement the annual fees/joining fees, late payments/delinquency fees, etc., as per the rules framed by the overseas organisation concerned. (www.rbi.org.in/guidelines) Residents are free to use ICCs for payments in rupees or foreign exchange for goods and services procured in India. Also personal remittances are permitted through ICCs subject to Exchange Control Regulations and compliance with conditions and documentation prescribed. ICCs issued in India are not valid for payment in foreign exchange in Nepal and Bhutan. Residents going abroad are free to use ICCs for all bonafide personal expenses, including the purchase of goods for personal use subject to their entitlements. The Baggage Rules/Exim Policy in force would govern import of goods so purchases abroad into India. The entitlement of exchange should be ascertained from the authorised dealer through whom reimbursement would be provided. Indian residents can draw foreign exchange against ICCs in the form of foreign currency notes/travellers’ cheques to the extent of their entitlement from an authorised dealer/full-fledged moneychanger. Sate of such foreign currency notes/travellers’ cheques out of entitlement would be governed by extent regulations and would be subject to the applicable ceilings and if applicable, be endorsed on the passport. Residents who have been issued ICCs and are going abroad for employment or on emigration are not permitted to use it for drawing exchange. They should surrender their ICCs before they proceed abroad on employment/emigration. They cannot be used for effecting remittances for the purposes for which release of exchange is not permissible under the extent of exchange regulations. Cardholders drawing exchange under BTQ against ICCs should on their return to India get their passports endorsed from the authorised dealers through whom the reimbursement will be provided. Returning Indians maintaining Resident Foreign Currency (RFC) Accounts in India or Foreign Currency Accounts abroad can also use ICCs freely without any end-use restrictions provided the
reimbursements are made by debit to their RFC accounts in India or foreign currency accounts held abroad. Non-residents are free to nominate any resident as additional/add-on cardholder and the claims arising out of use of such cards should be met by the non-residents from their foreign currency accounts maintained in India or abroad. However, there are some prohibitions on claims settlement by the add-on cardholder. EEFC facility is not available to the recipients in respect of payment received from residents against ICCs. Residents in India are permitted to ICCs arranged by overseas organisations provided liabilities arising out of use of such cards, in and/or outside India, are met by the organisation arranging the card. Under no circumstances remittance from India will be allowed to meet the liabilities arising out of use of such cards (Gupta, 2003).

4.5.2 United States Version

The consumer credit business in U.S is heavily regulated, both by agencies of the Federal Government and the individual states themselves. Federal Reserve Board (FRB) is the apex regulator that promulgates most regulations affecting consumer credit. The FRB has issued regulations regarding many statutes affecting the credit cards including Regulation Z, which implements the Truth in Lending Act; Regulation E, which implements the Electronic Fund Transfer Act; and Regulation B, which implements the Equal Credit Opportunity Act. Prior to 1968, the respective state laws solely regulated the consumer credit business. But after promulgation of the Federal statues in 1968, greater protection is available to the customer. (Gupta 2003). The major federal laws that affect bankcard operations in United States include the following:

(www.federalreserve.gov/publications)

i) Truth in Lending Act, 1968

The Truth in Lending Act (TILA), 1968 is the oldest consumer credit statute as part of the consumer credit protection act. The Federal Reserve Board (FRB) Regulation Z implements the provision of TILA. It governs opened revolving credit, such as credit card loans, as well as closed end credit such as mortgage loans. The purpose of TILA is to promote the informed use of consumer credit by requiring disclosures about its terms, cost to standardize the manner in which costs associated with borrowing are calculated and disclosed. TILA provides for mandatory disclosures.
According to its provisions, the card issuers must disclose specified credit card terms in a segregated box on or with each credit card. The disclosure must include information about the Card’s Annual Percentage Rate (APR), annual and transaction fee, minimum finance charges, balance computation methods, cash advance fee, late payment fees, over the limit fees, the grace period. Another disclosure known as the initial disclosure statement, must be made before the first transaction can be made on a credit card account. It generally accompanies the credit card agreement sent to the consumer. Also, the bank must provide the consumer with monthly billing statement that summarizes account activities and provides other basic information and a monthly or an annual statement of the consumer’s right with respect to billing errors and unauthorized transactions. The Act prohibits bank from distributing unsolicited credit card. As per Regulation Z, credit card can also be issued only in response to an oral or written request by the customer or when a customer submits an application for a credit card. However, a banker can familiarize the customer with the bank credit card offering and then issue a card if the customer requests it. The Act also limits a cardholder’s liability for unauthorized use of credit card to $ 50, and regulates the advertising of credit card terms. As a strict liability statute, a creditor is liable for any violation of the provisions of the Act and especially the penalties for the technical failures can be high. Consumers can recover actual damages they suffer plus punitive damages upto $ 1000 per occurrence. In a class action brought on behalf of many consumers, the group can recover upto $ 5,00,000 or 1% of creditors net worth, whichever is less. In addition, if the consumers prevails the court may require the bank to pay attorney’s fees and court costs.


The Fair Credit Billing Act (FCBA) requires investigating and resolving enquiries from consumers concerning alleged billing errors on their open-end credit accounts. Billing error includes inadequate transaction descriptions and the failure to mail a periodic statement to the cardholder’s address. Claims of the unauthorized transactions are handled separately. The Act requires a consumer to notify the creditor of the alleged error within 60 days of the mailing of the billing statement. Investigation and settlement of disputes and notification to the consumer must be completed within
90 days. While the dispute is pending, the creditor must refrain from collecting the amount in question and is prohibited reporting the cardholder’s account as delinquent to a credit bureau. Under certain circumstances the Act also allows the cardholder’s to withhold payment for merchandise or services if the consumer has dispute with the merchant regarding the goods and services. The Act allows a cardholder to withhold payment for any damaged goods or inferior goods and services purchase with a credit card if the purchase price exceeds $ 50; the transaction occurred has made a good faith to resolve the dispute with the merchant.

iii) Equal Credit Opportunity Act, 1974

The Equal Credit Opportunity Act, 1974 and Sub chapter IV of the Consumer Credit Protection Act prohibit discrimination in any aspect of a credit transaction based on race, colour, religion, national origin, sex, marital status, age or the fact that the applicant receives public assistance benefits or has exercised his or her right under another section of the Consumer Credit Protection Act. Each of these characteristics is termed as “prohibited basis” under the law. The Act also applies to both consumer and business credit. The regulatory demand imposed by the Act requires banks to carefully design and word credit application forms and thoroughly train their loan officers. It also require lenders to notify a consumer whose request for credit is denied. An adverse action notice must be sent within a prescribed time and must list specific reasons for the denial of credit/offer to supply the reasons upon request.

iv) Fair Credit Reporting Act, 1974

The Act refers to Section 624 of the Consumer credit Card Protection Act. It’s principle objective is to regulate the purpose for which credit reporting agencies are permitted to give out information about consumer from their files. The Act designed to improve the confidentiality and accuracy of credit reports, the law is enforced by Federal Trade Commission (FTC) and State Consumer agencies. Individuals may challenge and correct negative aspect of their record if they prove there is a mistake. Consumer may also demand statements explaining why they received certain negative marks. Congress passed amendments to the FCRA that went into the effect on Oct 1, 1997 which augmented consumer’s privacy rights and further protected the accuracy of credit report information. The Amendments made it a civil law violation for someone to
obtain a consumer report without a permissible purpose. It requires credit reporting agencies to ensure that credit information is reported accurately and to delete obsolete information after a prescribed time. It also allows recovery by the consumer for actual damages incurred. It requires that a credit card reporting agency must ensure that person requesting credit information about a consumer have a permissible purpose for receiving that information.

v) **Fair Debt Collection Practices Act, 1996**

The Act is a United States statute added in 1978 as Title VIII of the Consumer Credit Protection Act. Its purposes are to eliminate abusive practices in the collection of consumer debts, to promote fair debt collection and to provide consumers with an avenue for disputing and obtaining validation of debt information in order to ensure the information’s accuracy. The Act creates guidelines under which debt collector may conduct business, define rights of consumer involved with debt collectors and prescribes penalties and remedies for violation of the Act. It is sometimes used in conjunction with Fair Credit Reporting Act.

vi) **The Federal Bankruptcy Code, 1974**

The federal bankruptcy cases, which can be brought before the court (i) straight bankruptcy case, in which the court appointed trustee collected and liquidates the debtor’s non-Exempted property and distributes the proceeds the creditors, (2) wage earner plan (deferred payment basis) and (3) cases though corporate reorganizations.

A bankruptcy case begins with the filing of bankruptcy petition by the consumer debtor and an automatic stay goes into effect, preventing creditors by law from taking any action, formal or issuer should establish internal procedures for communicating information about bankruptcy cases to avoid penalty for impermissible collection efforts. Also, if both spouses are liable on a credit card account, the creditor can bring action against the spouse who has not filed the bankruptcy case. The debt incurred on the basis of fraud, false pretences or false financial statements are most troublesome categories. To protect the card issuers from this practice of debtiness bankruptcy Act, 1994 incorporated a provision that either charges or cash advances exceeding an aggregate of $ 1,000 and made within 60 days prior to filling for
bankruptcy are presumed to be non dischargeable i.e. the debtor cannot relieved from legal obligation.

vii) Electronic Fund Transfer Act, 1978

In the late 1960s, Congress recognized that the explosive growth in the use of electronic systems to transfer funds made it imperative that it clarify, and where necessary establish, the right of consumers who elect to take advantage of the benefits of these systems. Accordingly, Congress enacted the Electronic Fund Transfer Act known as Regulation E. Regulation E, among other things, limits a consumer’s liability for an unauthorized electronic fund transfer from his account and establishes procedures that a consumer may employ to remedy alleged errors that occur in connection with his account. Under Regulation E, the way to report errors is somewhat different than it is with credit cards. But as with credit card, financial institutions must investigate and promptly correct any EFT error that the cardholder report. For this cardholder have to write or call the financial institution immediately if possible, but not later than 60 days from the date of first statement that has shown an error. By giving the name, account number and explain why they believe there is an error, kind of error and the amount in question. The financial institution must promptly investigate an error and resolve it within 45 days. For errors involving new accounts (opened in last 30 days), Point of Sale (PoS) transactions and foreign transaction, the institution may take up to 60 days to investigate the error. However, if the financial institution takes longer that 10 to business days to complete its investigation, generally it must put back into cardholder account the amount in question, while it finishes the investigation. The financial institution must notify cardholder of the results of its investigation. If it finds no errors the financial institution must explain in writing why it believes no error occurred. On lost or stolen card cardholder liability is limited to $50 per card. On an EFT card, liability for an unauthorized withdrawal can vary likely, loss is limited to $50 if the cardholder notify the financial institution within two business days after learning of loss as theft of card. But loss as much as $500 if cardholder do not tell the card issuer within two business days after learning of loss or theft. If the cardholder do not report on unauthorized transfer that appears on statement within 60 days after, the statement is mailed to cardholder. The cardholder risk is unlimited loss on transfer.
viii) **The Right to Financial Privacy Act, 1978**

This forbids financial institutions from disclosing customer records to Federal Government officials except in response to a written authorization from a customer or a written legal demand. If a federal agency or financial institution violates the right to financial privacy Act, the consumer may sue for damages or to seek compliance with the law. If the contention is proved the Federal agency/financial institution is bound to pay the attorney’s fees costs to the petitioner. (www.ampsmartloan.com)

ix) **New York State Assembly-Consolidated Laws**

New York State Consolidated Laws have exclusively defined credit cards and other terms associated with the credit card business. For example “Credit card” means and includes any credit card, credit plate, charge plate, courtesy card, or other identification card, device issued by a person to another person which may be used to obtain a cash advance or loan or credit or to purchase or lease property or services on the credit of the issuer or of the holder. Similarly, the terms like Issuer, Debit Card, Secured Credit Card, Unauthorised use etc. have been a comprehensively defined. The Consolidated Laws provides a comprehensive guide on various issues pertaining to credit cards including issuance, advertising, reporting aspects and card issuers and consumers’ right, duties and liabilities. Section 515 of the consolidated laws deals with the issuance of credit cards. It provides that not withstanding any other provision of the Law, no person shall issue a credit card in violation of the provisions of an Act of congress entitled “Truth in Lending Act’ and the Regulations thereunder, as such Act and regulations may from time to time be amended. The issuance of a credit card in violation of the provisions shall constitute a misdemeanour. Section 520 deals with application forms or solicitation for credit cards. It provides that any application form or pre-approved written solicitation to enter into a credit card agreement mailed or communicated otherwise to the prospective buyer shall contain the important disclosures in a specified chart form like serial No., Annual Percentage Rate (APR) Variable Rate Index Annualized and Spread, Cash Advance Fee: Transaction Fee: Membership fee, Grace period for purchases, late fees and over the limit Fees. It also provide for mandatory disclosures like:
• Interest rates to be expressed as fixed APR. If the variable rate is provided, it should express the linkage to the index.

• Membership as participation fee shall be expressed as an annualized amount. If no such fee will be imposed, issuer shall indicate “No” or “None” or “Does not apply”

• Any cash advance fee, per transaction fee, late fee or over the limit fee that may be imposed shall be expressed as an amount or as a percentage of the transaction, as applicable. If no such fee will be imposed, the issuer shall indicate “No” or “none” or “Does not apply.

• Nothing prevents/prohibit on issuer from disclosing additional terms conditions, or information, whether or not related to the disclosures required under this section, in conjunction with the disclosures required by this section.

• Grace period if offered must be clearly mentioned.

• All application forms for a credit card agreement, including those in a magazine, newspaper, or other publication distributed by someone other than the issuer in this State on or after 01-01-88 shall contain a statement in substantially the form-

  “If you wish to receive disclosure of the terms of this credit card, check here and return to the address on this application.” If the federal law required the card issuers to comply with the stipulated requirements, the requirements of this section are deemed to have been complied with. Section 512 of the consolidated laws provides for *limitation of liability for unauthorized use of a credit card or a debit card*. It provides that a provision which liability upon a holder for a cash advance or loan or for the purchase or lease of property or services obtained by the unauthorised use of a credit card or a debit card, shall not be enforceable, to the extent that it imposes a greater liability upon the holder than is imposed upon the holder of credit card under the provisions of the Act of entitled “Truth in lending Act” and the regulations thereunder, as such Act and regulations may from time to time be amended. Section 516 provides that in any action brought by the card issuer against the cardholder in relation to a credit as debit card, and the cardholder object to such detention as action, it shall be a defence to such action that the person was detained in a “reasonable manner” and for not more than a “reasonable time”. Section 514 deals with Defences. It provides that in any action for a cash
advance or loan for the purchase or lease to property or services through the use of a credit card or a debit card, it shall be a defence that such obligation.

(a) arose out of the unauthorized use of a credit card or a debit card which was not delivered to the holder, or

(b) arose subsequent to the giving of notice by the holder to the issuer of the unauthorized use, loss or theft, of such credit card or debit card; or

(c) is in the excess of the limitation of liability for the unauthorized use of a credit card provided in the act regulations thereunder, as such act and regulations may from time to time be amended.

If any of the defences set forth in subdivision one of the section be established, the court shall order the issuer to pay the reasonable attorney’s fees incurred in the defence of the action if the court finds.

1. that the holder has co-operated with the issuer in determining the facts and circumstances relating to such unauthorized use, loss theft, of the credit card or debit card; and

2. that notwithstanding such Cupertino with the issuer, the issuer has brought the action without reasonable cause.

Section 517 provides that no agreement between the issuer and the holder shall contain any provision that a statement sent by the issuer to the holder shall be deemed correct unless objects to within a specified period of time. Any such provisions is against public policy and shall be of no force or effect. Section 518 prohibits merchant establishments from charging surcharge from the cardholders for card payment. It clearly states that no seller in any sales transaction many impose a surcharge on a holder who elected to use a credit card in lieu of payment by cash, cheque or similar means. Any seller who violates the provisions of this Section be guilty of a misdemeanour punishable by a fine not to exceed five hundred dollars or a term of imprisonment upto one year, or both. Section 519 deals with disclosure by commercial establishment honouring credit cards. Among other disclosures, it provides that all establishments that honour credit cards a pose conditions to acceptance or use must mention on the concerned advertisements. Any person violating the provisions of this section shall be subject to a civil fine of not more than $100 on the first violation and not more than $
250 on the second and all subsequent violations. (www.assembly.state.ny.US/cgi-bin/claws).

4.6 Cross-Comparison

Whereas India is soon becoming a country with the second largest number of credit cards in the world, it is a matter of utter surprise that India does not have a comprehensive legislation for cards business. The U.S., leader in terms of the number of cardholders has well defined set of legislation to protect the interest of the cardholders as well as that of the card issuers. Following paragraphs attempt to point out deficiencies in the Indian legal and regulatory framework vis-à-vis United States especially from the view point of the consumers:

i) Disclosures

In U.S., the federal statutes provide for a comprehensive clear-cut, mandatory user-friendly disclosure of the card issuing terms to the consumers/prospective cardholders. To quote, every application for solicitation of credit card should clearly indicate in specified format information about Annual Percentage Rate (APR), entry fee, transaction fee, over-the-limit fees and the grace period. However, in India this disclosure is more or less inadequate and only partial information is disseminated to the cardholders. Interestingly, the direct sales associates of a majority of card issuers are not fully aware of the card issuing terms specially the calculation of APR and balance computation methods. The consumer awareness level is undoubtedly, on a lower side in India. There is lack of published data on various important aspects specially the number of card issued, volume of business, cases of frauds etc. The RBI is far away from promulgating a concrete mechanism/ set of guidelines to cover this most important aspect of credit card business. There is no specific regulation for detrimental trade practices frequently followed by the card issuers, which they may indulge in given the cutthroat competition in the credit card market.

ii) Lost Card Liability

The Truth in Lending Act as applicable to the United States limits a cardholder’s liability for unauthorised use of a credit card to $50, and also regulates the advertising of credit card terms. However, in India, the offer terms of various card-
issuing banks in India provide a marginal relief to the cardholders. In some cases, the lost card liability is limited only to Rs. 1,000/- but in other cases it is unlimited.

iii) Liability on account of Technical failures

As a strict liability statute, the Truth in Lending Act provides high penalties for technical failures and consumers can recover actual damages they suffer plus punitive damages up to $1,000 per occurrence and in case of consumer groups up to $500,000 or 1% of creditor’s net worth, whichever is less. In addition, bank may be required by the court to pay attorney’s fees and court costs to the petitioner. In India, the rate of technical failures is very high especially at ATMs and generally, the card issuers accept no responsibility for such failures. Even proving such cases in the consumer courts is a cumbersome task.

iv) Card defaults

In U.S., the legal remedy for the card issuer is clear. The Issuer can seize the accounts of the credit cardholder and can file a petition for recovery of card outstanding in case of default.

Also, the existence of an efficient mechanism for information sharing between the card issuers helps the issuers to keep a track of consumer’s credit history which in turn helps reduces bad debts. The federal statues like Federal Bankruptcy Code, 1974 Fair Debt Collection Practices Act, 1978 etc. provide an efficient framework for recovery of debts and clearly define the rights of the consumers and the sellers i.e. the card issuers.

The Indian law does not offer a straightforward mechanism for the card issuers to deal with the card defaults. Apart from the in-house recovery teams for handling default, the issuer (debtor) can file a civil suit under the provisions of IPC. Garnished by the weak insolvency laws, the delinquency ratio base has been rising sharply making extremely difficult for the card issuers, especially for the Indian banks, to handle the problem. There is neither a clear idea for outstanding nor a common database to check defaulting clients. However, some steps have been taken to create a common database to enable sharing of information on defaulting clients. However, some steps have been taken to create a common database to enable sharing of information on defaulting customers.
v) **Grievance Redressel Mechanism**

The United States laws provide an exclusive mechanism to settle the grievances of the holders of financial products including credit cards. The law provides for an exhaustive definition of the various terms like credit cards, debit cards, Issuer, unauthorised use etc. as mentioned above, but in India no such definition of such crucial terms are found in any of the enactments. The Consumer Protection Act, 1986 suffers from serious limitations in relation to consumer justice.

vi) **Interest rates regulation**

The Banking Regulation Act, 1949 is limited in its scope and provides for regulation of financial products in general context. The interest rates on credit cards are presently deregulated which unfortunately places heavy financial burden on consumers. Though deregulation of interest rates have shown positive signs in developed countries, the Indian scene is completely different whereby consumers are far away from being tuned to the credit environment. However, for Smart Cards & Debit Cards, RBI has placed some restrictions on interest rates charged by card issuers.

vii) **Others**

The compulsory filing of Income-tax returns by the credit card holders under the provisions of Section 139(1) of the Income Tax Act, 1961 and treatment of expenditures made by salaried employees as perquisites under section 17(2) of the said Act Is posing a threat to the card business due to forceful disclosure of their incomes and consequently, high tax liabilities,

Also the stringent provisions of FEMA as applied to ICC holders are prohibiting the mass expansion of the card business.

Federal Statutes apparently provide for restraining financial institutions from disclosing customer records to federal government officials except under legal demand (as per the provisions of The Right to Financial Privacy Act, 1978). In India, there is no such exclusive legislation.

Hence, there is a need to explore the various legislative premises of the inferior and unclear Indian version for protection of interest the credit card holders and the healthy growth of the industry.