Critical Analysis of Credit Card Frauds in India

Anuveeta Datta Chowdhury[1]

ABSTRACT

With an advancement of green revolution and with a global challenge to making less use of papers, the Indian financial system has shifted to Online banking transactions. Online transactions have many benefits like saving of time, papers, hazards etc. but the cyber-crimes are rapidly increasing in banking sectors through the media. The research paper covers different types of credit card frauds in India. The paper also focuses on lack of Governance of Reserve Bank of India in Online banking transactions. The liability of banks and cardholders in such cyber banking frauds are the main issues to be dealt in this paper. The research paper discusses how Criminal law is implemented in credit card frauds. The concept of plastic money has made customers shifted towards online banking transactions..The credit card payment defaults have contributed much towards banking frauds in India. There is grey area prevalent in law between default credit card payments and customer's willingness to pay in any other mode. The research paper has highlighted the critical issues of credit card fraud investigation techniques. Mainly three relevant Indian Statues have been referred in supporting the different factors of banking frauds in the paper, namely The Negotiable Instruments Act,1881, The Indian Penal Code,1860 and The Foreign Exchange Management Act,1999.

The purpose of the research paper is to resolve the research question about the liability of banks and card holders in banking frauds. Law operates not in vacuum but in prominent governance of Reserve Bank of India and protecting the finances of customers of banking sectors has become one of the concerned issue of the day. The present paper undertakes doctrinal and analytical research methodology to critically examine the impact of the online transactions in banking sectors.

Keywords*: Credit cards, Online transactions, liability, fraud detection techniques, cyber-crimes.*

I. INTRODUCTION

Fraud can also be defined as trickery, willful deceit or spurious thing. Fraudulent activities can be traced as long as mankind existed. Fraudulent ways are evolved with time and keep evolving. New inventions are giving newer ways to fraud every day. The challenge to find the loopholes in any system and to use them for personal gain or benefit. An opportunity to event established norms and the notion right or wrong is kind of criminal

[1] *Author is a student of University of Petroleum & Energy Studies, Dehradun*

thinking and is capable of provision from law enforcer. Nowadays the card issued on their part have wings family in order to improve and improvise on existing card features in order to make them fraud proof. But still the features of a module function one that for the identification of proving that the present of the card is genuine and the other that of proving that the card is a genuine card. Both together make a secure mode of payment. But actually it lacks to provide secure mode of payment.

The concept of attempt is one of the most intriguing and integrate problems in criminal law. An attempt to commit a crime is basically an act done with intent to commit that crime and forming part of a series of acts which constitutes its actual Commission if it were not interrupted. The Indian Penal Code Amendment Bill yet to be passed has added the additional section 120 C which defines attempts as follows;

'Person attempts to commit an offence when he with the intention and knowledge requires it for committing it does any Act towards its Commission, that so done is closely connected with and proximate to the commission of the offence and the experience in its objective because of facts not known to him or because of circumstances beyond his control.'

II. TYPES OF FRAUD

Application fraud

The fraudster obtains all information of a person who would be eligible to get a card. Hidden applied to the issue with that person's information except for the address. The issuer will issue the card based on the information of person without the person even being aware of it. A variation of this product is that the product obtained the card details of the genuine card holder. He then calls of the issuer pretending to be the genuine cardholder to report his card as lost and to request the issued to send the card at a new address. If the bank does not call up the card holder to confirm or to verify the change in address, the fraud star will get a genuine card on which we can run up whopping bills.

Lost or stolen fraud

Any cardholder can lose his/her card in Shops, movie theater and ATM which can be then stolen by a thief and misused to purchase expensive items which can later sold in market for quick and easy cash. People suffers such kind of frauds day after day.This information, normally be used in multiple ways in order to defraud the issuer at a later date at Fraudster's convenience. He uses the card at the merchant shop for a single transaction and allows multiple imprints of his cards to be taken. The Merchant submits this imprints with forged signatures and obtained his payment from his acquirer. The Merchant has already been played on the card holder refuses to pay, it is the issue or who has to bear the fraud loss. It is difficult to prove such collusion until and unless the same cardholder keeps appearing in many such cases of fraud.

Multiple Imprints

The fraudulent merchant may ask a gullible card holder to sign or more than one charge slip on some pretexts ,such as print is not clear on the present charge slip on the signature on the chart slip does not tally with that on the signature panel of the card. The Merchant in presence of these consecutive charts leave to his Acquirer in the gap of a few weeks or even months. The merchant makes payment because on the face of it everything the signature imprint it seems to be in order. The cardholder cannot deny the charges since he has himself signed on the charge slips. The rule of game is you signed for it now you have to pay for it. Any denial from the cardholder's part however will not diminish his liability. He will be asked to pay his dues first and if the proof is proved and the money recovered the issue will repay the card holder the amount by which he was defrauded.

ROC Pumping

A merchant with fraudulent intention takes more than one imprint of cardholder's card on the imprinter. The Exclusive provided by the path sent to the card holder for taking more than one important is that the earlier important is unclear. But more often than not the card holder does not ask why more than one imprint has been taken. Many a times the cardholder is aware of the procedure involved for acceptance of the card by the merchant. Frequently the importance and not taken in front of card holder has in case of restaurants where to sign for the bill and provide your card to be taken by the waiter for billing and the checkout clerk main take the car to another cubicle across the counter for another imprinter.

Once the merchant has the imprints of the charge slips, he then just the card holder signature from the original charge slips and presents the charge slip to the Acquirer after a gap of few weeks at least

Sold paper

This is a kind of variation of ROC pumping fraud. The issue was caught on to the fact that when merchant submit executive charge slips for the same card holder at an interval of few weeks or even months it would be more often than not to be a case of fraud. And presenting the charge slips after such a long period means and in ordinate delay for the merchant in getting his money. This is more difficult to trace. It is known as soul paper frauds in some paper that is the charge slip is sold to other merchant for a fixed price. Merchant is then free to feel in any amount before submitting the charge slips to his Acquirer.

White Plastic

White plastic fraud is fraud perpetrated by using a black piece of plastic. The gang uses credit card information which has been downloaded from whose terminals obtained through their contacts in credit bureaus or at the issue words by embossing the plain blank pieces of plastic. By colluding in with the fraudulent merchants against fraud star can take as many in prints of the various cards he wants for any amount that he feels is right

for the signature on the charge slip and have them presented to the Merchant. It is not difficult to identify that the important is that of a card because the embossed figures of the card pin number are bound to be crooked and will not follow the same found or pattern of the original card.

Generally, fake cards are manufactured using sophisticated machinery and Imprinters are used to give unsuspecting merchants. Many a times fake cards are used as identification or documents proof. The question is whether this would constitute a credit card fraud.

In the case of ***United States v. black mon[2],*** the difference fake credit cards for the purpose of identification. The court held that days did not constitute a credit card for under 18 USC section 10 29 A3, because these two violate this section, there must be an intent to different a credit card holder for a credit card company or Bank. While using the credit card as false identification is not sufficient to be liable[3]

Card number

Though the card might be valid for a long time after it is stolen or lost it might be reported in the warning Bullet in as a lost or stolen card. A merchant has to go through the warning Bulletin before he accepts the card as valid and gives goods to the card holder. The very fact that the card number does not exist in the morning Bulletin is considered as sufficient proof that the card is not lost or stolen. A slight alteration in one or two digits of the card number can make it a clean card and can be freely used by the fraudster.

Signature panel

The original signature panel of the card with original card number is ripped off and replaced with another signature panel which has the altered card number printed on it. The added advantage being that the signature panel is not blank and can be signed on by the fraudster in any way he is comfortable with. He need not use the services of a food that every time he wants to use the card.

The original signature panel will have the name of the issuing body like visa, master Discovery accept printed across the background of the signature panel. The card number is also printed in a unique stylist font. It is difficult for a fraudster to imitate both the background print as well as the stylish lettering on the signature panel.

Magstripe

This kind of frauds can be perpetrated where the Merchant has an imprinter but not an EDC terminal. Terminal is wild card holder in which reads the information from the magnetic stripe embedded in the card. This

[2]839 F 2d 900(1998),

[3]Rupa Mehta &RohintonMehta,'Credit Cards: A Legal Guide (with special reference to Credit Cards Frauds',Universal Law Publishing Co

magstripe has information about the card number its expiry date and other card holder details. When that card number and signature altered but the magstripe is not touched the anomaly between the card numbers and the original is evident. The cardholder immediately be supported as a false card been used fraudulently. In order to avoid this the fraudster, demagnetizing is a mathematical trick and encodes it with fresh data which will match the alterations carried out on the face of the card.[4]

Carding

When a card is stolen the thief does not know if the card will be valid when he makes his big purchase. If a card holder has reported it lost or if the card limit is already completely used up the card is useless to the thief so how does that you find out data card is still good for use or not. The thief uses the card for purchase on the net preferably to make a small donation to a charity.

The thief chooses the option of Charity because you don't have to provide the shipping address to a charity also he doesn't have to waste time search in items that are small value in a for his purpose. The amount is kept small so that the limit is not used up too much and also because a large amount to be in all probability attract attention of human reviewer. Carding is also used when credit card data obtained by scheme in our fishing in order to verify whether to obtain data is valid or not. Once the data is verified, the card will sell the data to other Fraudsters, who will carry out actual fraud for amounts that vary depending on the freshness of the data status of the card and type of the card.

Phishing

This kind of fraud is an email scam where the first lead to the card holder to believe that he is responding to a legitimate email request from unknown or well-knownorganization.

The way this scam works are the followings:

i. Card holder receives an Email from a well-knownorganization Bank except requesting him to update his personal information for security reasons for updating the existing records.

ii. The fraudstarensure that the site looks as close to the genuine site as possible including the logo company name address etc.

iii. The email will have a link which the card holder will be directed to click on for updating the records.

iv. When the card holder clicks on the link, he will be asked to feel about a short form giving his personal details such as name address card number pin CVV number.

[4]Ibid 1

v. Mini unsuspecting cardholders provide information believing that they are responding to their own bank or some known Merchant

vi. Fraudsters get this data and use it to transfer funds into their own accounts on to buy goods online which they cancel later.

By the time the cardholder realizes that he has been duped, the fraudsters have made away with the money and goods. Some fraudsdo a step further, when they request the recipient of the mail to download and install a security software that will protect them. If the software is installed the fraudster can monitor the computer and capture card and bank account details. The spam email itself is sent from unsecured computer or server that fraudster has taken over.

To protect oneself from becoming a phishing victim, the following steps should always be borne in mind: -

- Banks merchants of Financial Institutions do not ever request customers to send sensitive information such as passwords or pins online.
- If you receive such a mail always pay special attention to the name of the organization address logo on the URL address in some in it with determination to find a mistake.
- Preferably access your bank card issued science by typing the address on the web browser rather than clicking on link, however easy it may seem to do so
- If you receive such a mail, notify the bank issuer immediately
- If you receive such a mail go to the bank and the issue immediately
- Most important is to check your financial statements when they arrive for any discrepancies and to notify the authorities if you do not find any such statements.

ATM Fraud

ATM fraud includes both trapping and operational fraud. Trapping is simple and the thieves do not need the card order data. There are tricks 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 from outside. The unsuspecting cardholder keys in his details and punches in the amount that he wants to withdraw. The transaction process and dispensing of the notes which is win the notes get stuck. When the note got stock the customer public works server to another ATM to withdraw to complain. The thieves' keeper watch when enough number of customers have walked into withdrawal come in and clean the ATM. Trapping alone has resulted in a loss of millions of euros in Europe.

Operational Fraud

In this action games into any banks ATMs administrative privileges. The thieves do many things one of them being he can choose to be programmed ATM to think that is loaded with a hundred rupee notes instead of 500 rupees notes. Whenever any customer will want to withdraw rupees 500 ATM will dispense 500 notes instead of just one note of 500. In all probability the hacker himself will have an account with this bank.

III. CREDIT CARD FRAUD DETECTION TECHNIQUES

The credit card fraud detection is the uncovering of fraud symptoms either in circumstances where no prior suspension exists or in circumstances where there is some sort of doubt. Detection is done through a safety valve a systematic apparatus. Is the right way and kind of duty of every credit card issued by the bank otherwise to install proper comprehensive and simply detection system in its operation of the credit card business. After erection system and institution about impending dangerous and just perpetrated frauds such that a molehill is demolished before it becomes huge mountain.

The banking corporation has an obligation to its client's shareholders creditors and society at large to install and in fuse and ongoing and relevant system of detection which is of such form and content that it was lead to investigation and recovery of Loss funds or to prompt knowledge about impending fraud. In the world of credit cards fraud detection techniques strive for the detection of symptoms of text manipulation misrepresentation collusion and concealment.

IV. CONSISTENCY AND CONTINUITY

Fraud detection should never be one of exercise it should rather be an ongoing and routine aspect of the credit card banking business. Now this consistency and continuity are already sometimes mistake in as spin off from conventional audit or internal audit but as a specifically designed detection arrangement with specific resources and systems assigned on a continuing basis from year to year.

Prevention is better game in banking business

The proverb says that prevention is better than cure. The objective of fraud detection is and must always be prevention and at times even deterrence. Actually the difference follows each investigation properly persuade to its logical and the Convection and punishment of its perpetrators. The value of detection system in place have to be gauged not just by the number and quantum of cases of fraud solve but the unknown and at times and unknown dodge figures of roads that were not for perpetrated due to different effect of the system.

Prevention goes hand in hand with deterrence. Credit card companies have become more ingenious and resourceful in devising fraud protective measure such as identification cards signature card, smart cards,

computer software etc.To detect fraudulent use of cards, methods currently used include video recorders at ATMs and biometric identification which takes the form of reference to some physical attributes unique to the cardholder such as fingerprint or Iris configuration. The high cost of these measures is the main reason for the slow implementation of these techniques in banking business.

Responsibility and Accountability

Every task in operation of the credit card business must have a clear delineation of both responsibility and accountability. Most Fraud Escape detention usually because no what is made accountable for the task. Thus the assignment of responsibility and accountability not only allows the investigators to pinpoint quite easily who must be the prime suspect but also puts the person so responsible or accountable in a position such that he decides to avoid perpetrating a fraud. Therefore, designing of responsibility and accountability not only deters but also prevents.

Generally, flowing from the practice of assigning responsibility and accountability is the Thumb Rule that wants investigation has identified that a particular employee was involved in the copy tradition of a fraud either singly or in concern with some other person the said employee must be punished.

It has been observed that to punish or to fire a very good or trusted employee in such a case of fraudulent transaction has been very difficult decision for the organization. Organizations are generally frightened of publication of these fraudulent transactions incidence in public which will repeal their customers from investing in their organizations. But the punishment must be certain Swift and must be properly published so that every employee must think twice before engaging in such for different transactions.[5]

Zeroing in on crucial functions

Within the credit card operation there are certain hotspots of potential honorable fraud opportunities. The preventive system must make it certain that those potential vulnerable positions are not only men it properly but also routinely monitored. Position such as card acceptance, authorizations embossing cards are potentially vulnerable from the point of view of roads being committed by those manning them in Collusion with outsiders. These positions must be suitably staffed and monitored. Not only the staff chosen be more than honest but they must be periodically transferred to other high fraud risk operations. This has a dual advantage for sleeve do not allow sufficient report to be built between the employee and the outsiders due to a long-term.Mannering of a vulnerable post and thus reduce chances of corruption and fraud and secondly it brings a new more than honest in place of another more than honest and therefore expose the mistakes if any of the outgoing of previous concerned authority.

[5]Bank Guarantees in International Trade, Fourth Edition, Roeland F Bertrams, Wolters Kluwer Law &Business, ICC

The vulnerable post must be subjected to surprise and objectively conducted random test by a special team of investigators. This team of investigator should look on to the activities of high risk transactions made by the employees of the organization. This special audit may be a special unit from within the banking corporation outside professionals employed for this very purpose

Areas on to which zeroing in can be done within the credit card industry all branches remote from head office coma single Occupancy offices, what areas shared by one other persons such as embossing areas, persons to improve and advances to clients, employees authorizing electronic funds transfer on the card, officers controlling sensitive business information, managers who write of Debt example collection manager. This kind of zeroing in is called function based zeroing in. There is another type of zero in in which is called personal characteristics zeroing. There be investigated or departmental manager looks for certain triggers or danger symptoms within the employees or staff that he manages.

This fraud danger symptom includes high cash pending, unexplained wealth unhappy and disgruntled employee different kind of vices like heavy drinking, horse racing, gold buying, playing in stock interest in other competitive businesses, frequent absence for spurious reasons, friends or relations employed in or operating competitive businesses, excess financial commitments, close social or personal relationship with suppliers and lack of company loyalty.These indicators must never be ignored as they lead to a treasure trove of fraud.

Brainstorming as detection technique

Senior managers of credit card issuing Bank can come together occasionally to discuss informal in a relax atmosphere the various specifications of fraud opportunities. Idea leader's analysis should be conducted by a group of trusted employee's different skills and must include discussions on at least the followings like Assets at risk, method of theft, method of concealment, method of conversion, method of Collusion.

Maximum possible loss, one of versus systematic Road, organized crime and repulsion sharing information on departmental basis of frauds already on earth, identifying computer rest, effectiveness of controls, identifying potential thieves.

Employee as the detector

Detection of fraud is not necessarily domain of departmental managers, external and internal auditors, private investigators are the police. The most logical thing to do but Indeed it is very difficult as it is the development of information sources within the corporation itself. When you have a failure employee be a company in format is very difficult because most employees are Pro employees rather than Pro management and feel that if they turn in formers they will be stunt and ostracized by their own. It is indeed a fact that most direct attention to have the employer became the informant are prone to failure. However, what must be attempt is to take the

complete stuff into confidence and build a sense of toilet is such that they automatically informed about dishonest colleagues. This is easier said than done but many corporations have succeeded in encouraging all staff members to be aware of the possibilities of fraud. In this regard a system of annoying reporting of suspicious behavior has worked well do they have been at times was used to cast a cloud of doubt upon an employee particular leaders light by the anonymous complaint maker.

V.INTERNAL INTELLIGENCE GATHERING AND STATISTICS

Internal reports statistics and intelligence gathering is the base on which the header files of the fraud investigation team are build up some of the important aspects of the issue includes

- An extension of this approach is the employment of an Undercover agent this is normally done to cover extension ongoing and incremental frauds
- Early warning system or early recognition system
- Getting updated with fraud trends
- Proactive fraud control methods
- Surveillance cameras at ATMs
- Proper, methodical and perfect credit card documentation
- The internal investigation team will depend a lot upon the quality of the documentation generated and recorded. The internal investigation team will depend a lot upon the quality of the documentation generated and recorded by credit card issuer. Many a times this documents could give important leads to the resolution of fraud such as address of a customer his car number his telephone number,

some of the more important documents are the following

- Receipts
- Letters written by card holder
- Authorization logs including day, date time of withdrawal and authorization.
- Card holders billing
- Original card application.
- Charge slips.

Internal Red flagging and caution signals

Vigilant internal investigation team relates largely upon computer control danger signals are what we called red

flags. For example, the computer maybe program to give a monthly report on the various merchant establishment where frauds have been taken place. Now if a particular merchant establishment is repeatedly shown as a place where frauds are taking place for out of proportion with frauds taking place elsewhere than a fraud investigation team immediately investigates that particular merchant establishment thoroughly.

Similarly, the computer should be gathered and program to immediately draw the attention of the fraud investigation team if abnormal credit card transaction or activities are noticed. For example, if a particular card holder habitually spends between 2000 and 5000 a month and suddenly in a particular month is pending is 10 times of that amount then the computer should Road redemption of the bank to this fact which may require immediate investigation. In a particular vein,when too many transactions are being transacted at ATM machines order jewelry shops then again the computer will draw attention the card issuing bank which way necessitate investigation.

Data on direct sales agent(DSA)

Data on direct sales agent procures business for the card issuer. In short, it is outsourcing of marketing and sales. A proper investigation control of the DSA can bring to light the rate of the fraud of clients to whom cards were sold by a particular DSA. Does if the rate of fraud and delinquency is much more of clients who have been sold the card by a particular DSA, then this fact need investigation and rectification. Similarly, at times a particular DSA may be very good honest and efficient but may have a fraudster in the employment of the DSA as it sale.

Internal investigation

Tape recording is very beneficial in investigation but video recording though optional is also a great weapon, in the prosecutor'sarsenal. Internal investigation refers to the investigation of the credit card fraud by the personal of the credit card issuing Bank. Internal investigation has two aspects, firstly internal investigation maybe to actually investigate the fraud perpetuated in the stated case. Secondly internal investigation could be an investigation of such a nature which mitigates the possibility of the said fraud continuing. It is needless to say the two Prime reasons for conducting internal investigation is to reduce the quantum of the fraud and to attempt to pin point and apprehend perpetrators.

Specialist Fraud Investigation Team

The fraud investigation team consists of specialist. The team members have specializedknowledge which they have a quit due to longevity in the said function. If past is preload and if history teachers are asked in the past experience of the fraud investigation team is very crucial in attempting to unearth the unseen future, a fraud. Fraud investigation teams are aware of situation and can analyze typical *Modus operandi*of the fraudsters. They

have with them readymade best practice templates. Does the fraud investigation team also buildsover a period of time a good report and understanding of the workings of the police department specially the economic crime unit and criminal investigation department.[6]

Networking with Competitors

The fraud investigation team works continuously with competitors to understand repetitive forms of fraud and fraud perpetrated by the same person or by gangs. Almost all major internal investigation begins with calls to the other credit card issued to try to get leads of the case in question.

Short Reaction Time

The investigation team should react in the shortest possible time as in in these kinds of Corporate crimes loss can be controlled and apprehend the perpetration. The first step that a fraud investigation team needs to take, when the card is reported loss is to immediately put the card on pick up and in the morning Bullet in which simultaneous communication to authorizations and blacklisting the card in the system. The Merchant establishment must immediately get in touch with investigation team if the card which is lost or stolen card is attempted to be used. The attempt of use of card is important as habitual offender can be traced in this ways. The fraud investigation team must make attempts to ensure that merchant establishment delete the transaction and what does not part with the said card back of the person attempting to use it. Many a times a quick reacting internal fraud investigation team is able to represent of fraudstar with the help of the merchant establishment by delaying the transaction and in the meanwhile present in the fraudster other with the help of the merchant establishments, internal security guards and or the normal police[7].

VI. CREDIT CARD AND THE CRIMINAL LAW –INDIAN PENAL CODE

Types of Fraud	**Laws/Section**
Application Fraud	Attempt to cheat (Section 511 read with Section 415)
	Attempt to cheat by personation (Section 511 read with Sec 416)
	Attempt in commit offence in abetment to cheat(Section 511 read with Sec 508 ,)

[6]John K Villa,'BankingCrimes',Thomson& Reuters

[7]Johanna Niemi, Iain Ramsay and William C Whitford,'Consumer Credit, Debt & Bankruptcy: Comparative and International Perspective', Hart Publishing, Oxford and Portland, Oregon,2009

Stealing a credit card	Theft(Sec 378)
	Theft by clerk/servant(Sec 379)
	Abetment of Theft(Sec 307 read with section 378)
Misuse of Credit Card by credit card holder	Theft (Sec 378)
	Cheating (Sec 415)
	Cheating with personation(Sec 416)
Selling stolen Credit Card	Receiving stolen property(Sec 411)
	Receiving stolen property in commission ofdacoity(Sec 412)
Credit Card Fraud perpetrated by forged signature	Forgery(Sec 463)
Credit Card Fraud perpetrated by Gangs	Criminal Conspiracy (Section 120A)
	Acts done by several person in furtherance of common intention(Sec 34)
	Abetment of theft by Clerk/Servant(Section 107 read with section 379)
	Abetment of cheating (Sec107readwith 378)
	Abetment of cheating by personation(Section 107 read with 416)
Making a counterfeit Card	Forgery(Section 463)
Dishonor of cheque given by card holder to Bank	Section 138 of Negotiable Instruments Acts.

VII. THE LIABILITY OF BANKS AND CARD HOLDERS

The business of Credit Card, Debit Card and ATM cards includes numerous and various types of accounting and scenario which impose diverse kinds of liabilities upon banks and card holders.When a Situation arises in cases where the card holder has made the payment to the bank but the bank has not paid the money whatever the reasons are. The law does not provide any clear distinction between completion of the payment transaction itself and the discharge of the underlying obligation.A Bombay High Court ruled that a summary suit was maintainable in connection with issues concerning credit card facility by a bank and dispute regarding its users.

In this case the Court ruled that

- when the holder of a credit card uses the same, he agrees to comply with the terms and conditions of the credit card agreement
- when the credit card holder signs the slip at the shop or outlet, he acknowledges the amount due and payable
- by using the card, he does not pay the seller but to pay to the credit card issuing Bank along with other charges, if any which are gulliable.
- a suit based on the use of credit card is maintainable as a summary suit

The principal guiding us is quite clear under common law that when a debtor (card holder) owes amount under the number of debts, unless he specifically expresses how a payment should be approached in payment of those debt the credit bank is able to appropriate any amount as he wishes. Thus, the card holder may owe the bank debts on various counts, such as Annual fees, interest charges, cash withdrawal, purchase etc. but when he makes a payment without specifying expressly which particular that he is paying for, then it is the prerogative of the bank to appropriation it to a particular debt or to the general totality of the debt .[8]

Liability of card issuing bank and the supplier

In the landmark judgement of Recharge card services, (1988) 3 All ER 702, what's that a credit card issuing Bank was liable to pay the supplier (shop)irrespective of whether the debtor (card holder) is able to pay the creditor. Does the creditor take risk as long as the amount of the serious below the limit of the merchant establishment(shop). The same time another classification brought in by the decision that a Credit Card payment is absolute and not conditional payment for the supply of goods or services by the supplier that is the

[8]Deebey v Llyods Bank Ltd.(1912) AC 756

Merchant or the store. From the time of accepting the card as payment the supplier could no longer look to the card holder for payment, the supplier has agreed to look only to the creditor that is the bank.[9]

VIII. CONCLUSION

Prevention is better than cure and Safety must be maintained by the card holder as well as the creditor or the Bank. It must be ensured by the operative that the voice especially of the merchant are properly recorded if they are used as evidence.

The detectives must be properly trained in the conversation aspects of the string search that the merchant response are incriminating and self-damaging and are such that other values in Merchant and accomplices can also be roped in. The evidence collected is then passed on to the prosecutor for his used in obtaining a convection. Evidence collected is been passed on to the prosecutor for his used in obtaining a connection. The string mass optimally be given proper media coverage for that has a tremendous detained effect on other would be merchant Collusion fraudsters.

[9]Ibid 1