The potential of technological innovation to reduce fraud and increase trust in the Indian banking system

Dissertation submitted in part fulfilment of the requirements for the degree of MBA-Finance at Dublin Business School

BY

[Subhajit Routh]
[Student ID: 10402913]

Dublin Business School
Declaration

I, Subhajit Routh, hereby declare that this dissertation is the result of my own research hence every word so written is by me along with all details. All the sources are attributed and cited to their authors. This dissertation is solely meant for Masters of Business Administration in Finance and will not be a part of any other academic award.

Signed: Subhajit Routh

Dated: 26.08.2019
Acknowledgement

The success of completing the dissertation is incomplete without mentioning the name of the people whose constant guidance and encouragement made it possible.

I express my earnest gratitude to my Dissertation Guide, Mr. Andrew Quinn, for his constant support, encouragement and guidance. I am very grateful for his cooperation and his valuable suggestions. It would not be possible to make this dissertation without his cooperation.

I express my gratitude to all the participants who contributed in this research.

Finally I would like to thank my family specially my parents for supporting me. It is because of them that I learned the value of a human being.
Abstract

Everyone deposits their hard earned money with the banks with a hope that they can withdraw their own money on demand. Because of the technological advancement, alternative channels like online banking, mobile banking, ATM etc. fulfills their banking needs. This transformation has opened a new door of opportunity to the fraudsters, who are using newer techniques with malware, virus, ransomware to steal the public money from the bank, because of which customers are losing confidence on the banks as a safe keeper of their assets.

The main aim of the first and second part of the research is to find out the new techniques of committing online fraud and the technological innovations to prevent the same in Indian banking system respectively. The third part will propose the research methodology. The final section explains the outcome of the primary data which is collected by taking five interviews from senior bank officials.
# Table of contents

1. Introduction ................................................................................................................. 1  
   1.1 Overview of the study ......................................................................................... 1  
   1.2 Background of Internet banking and ATM banking ........................................ 2  
   1.3 Rationale of the topic ......................................................................................... 2  
   1.4 Problem statement ............................................................................................ 2  
   1.5 Research aim ...................................................................................................... 3  
   1.6 Research objective ............................................................................................ 4  
   1.7 Research Question ............................................................................................ 4  

2. Literature Review ........................................................................................................ 6  
   2.1 Literature Review 1 ............................................................................................ 6  
   2.2 Literature Review 2 ............................................................................................ 8  
   2.3 Literature review 3 ............................................................................................. 9  
   2.4 Literature Review 4 ........................................................................................... 13  
   2.5 Impact on customer behavior ............................................................................ 15  
   2.6 Alternative avenues for the consumers ............................................................ 16  
       2.6.1 Stock Market ............................................................................................... 16  
       2.6.2 Mutual Fund ............................................................................................... 17  
       2.6.3 Gold ........................................................................................................... 18  
   2.7 Implication on the banking system .................................................................... 19  
   2.8 Latest methods to commit frauds ...................................................................... 21  
       2.8.1 Black box attack ......................................................................................... 21  
       2.8.2 Man in the middle attack ........................................................................... 22  
       2.8.3 Ransomeware attacks ............................................................................... 22  
   2.9 Latest technology to prevent fraud .................................................................... 23  
       2.9.1 Blockchain ................................................................................................. 23  
       2.9.2 Neural network ......................................................................................... 24  
       2.9.3 Artificial Intelligence ................................................................................ 25  
   2.10 Application of technology in Indian banking system ....................................... 25  

3. Research Methodology ................................................................................................. 27
3.1 Research Methodology.................................................................27

3.2 Research Design.............................................................................27
  3.2.1 Research Philosophy.................................................................28
  3.2.2 Research approach.................................................................29
  3.2.3 Research strategy.................................................................30
  3.2.4 Research Choice.................................................................31
  3.2.5 Time Horizon........................................................................32
  3.2.6 Data Collection method.........................................................32
  3.2.7 Sampling...............................................................................33
  3.2.8 Research ethics......................................................................34

3.3 Research Limitation......................................................................34

4. Data analysis....................................................................................35
  4.1 Methodology of research............................................................35
  4.2 Participants Information.............................................................36
  4.3 Interview..................................................................................37

5. Discussion and conclusion...............................................................44

6. Personal Reflection........................................................................50

Bibliography.......................................................................................53

APPENDIX.........................................................................................56
List of Figures:

2.1 Components of ATM machine

2.2 Two way step to prevent ATM fraud

2.3 Workflow of Two way step to prevent ATM fraud

2.4 Stock market return of 20 years worldwide

2.5 Growth of Indian mutual fund market

2.6 Growth of retail and HNI customers of mutual fund

2.7 Share of mutual fund vs bank and insurance

2.8 Growth of different asset class over 10 years

2.9 MCLR rates of banks in India

2.10 Workflow of block chain process
Chapter I

1. Introduction

Over a decade, electronic fraud has been a major problem in the Indian payments system. In addition to being costly, the offence is believed to have been used to support other crimes such as terrorism. Efforts have been made to address this issue by the technological innovations. This research focuses on highlighting the consumer behaviour on trends and prevention method in electronic fraud in the Indian payment system. In 2017-18, alone Rs. 41167 Crores (almost $6 billion) worth of fraudulent transactions had taken place in Indian banking system. Between April and December 2017, nearly 24,000 fraud cases related to electronic frauds were registered in India. India was ranked among the top 5 countries with regard to credit card fraud. (Business Today; 2018)

A robust financial and banking system helps in overall improvement in the production of goods and services of the country. That is the reason why, Reserve bank of India (RBI) which is the regulatory bank of India has come forward to counter the problem. RBI has set up a fraud monitoring cell. RBI has come up with “too big to fail” concept which has also been helpful fraud prevention. Reporting of frauds have to be done by guidelines given by RBI. It has also stressed on the whistle blower policy to reduce the fraudulent transactions. On the other hand, banks are also adopting newer technologies to counter this ever increasing problem. The banks now a days working on blockchain technology, data mining process, neural networks, artificial intelligence etc. to detect and prevent this threat.

1.1 Overview of the study

The world has experienced massive improvement in technological innovations since 1990 which in turn changed the spending habit of the consumers (Bartling & Friesike, 2014). Today bank customers do not like to go to the bank to withdraw cash and then purchasing thing. They now prefer to use online banking, mobile banking, ATM banking to fulfill their transaction needs. It is also true that the business world has taken the advantage of the commercialization of “World Wide Web” to provide products and services quickly to the consumers. This changed behaviour has opened a gateway for the fraudsters, hackers to do the fraudulent transactions online (Douglass, D.B., 2009). In India also the same behaviour is witnessed, on the back of digitalization. Government is also encouraging digital payment policies to stop tax evasion and
encouraged in introducing several mobile wallets like paytm, airtel money, jio money etc. Major Indian banks have also joined the technological revolution by introducing mobile apps.

Earlier fake note, stolen cheques, forged signatures were used in making any fraudulent transactions, which could have been detected and prevented manually. But the technological advancement has made the methods of doing frauds complicated. Today hacking, phishing, pharming, vishing, smishing, skimming etc. have become the newer ways to commit frauds electronically. Even interbank transactions via secured network of “SWIFT” is not free from the attack of the hackers.

Fortunately there are technologies available with the banks to create fortress around vital assets. These new solutions are in part evolutionary versions of technology that has been around for a number of years, as well as new ways of looking at the problem of fraud through dynamic analysis, and even non-technology processes that turn those individual walls into gated communities.

1.2 Background of Internet banking and ATM banking

As the result of technological revolution alternative channels of banking have become more popular than the traditional channel. Evidence suggests that usage of digital banking in developed countries is more than 90 percent and diffusion of digital channels in developing countries range from 11 percent to 25 percent. The formation of National Payments Corporation (NPCI) in the year 2009 has set the stage for development of retail electronic payments which offers enormous opportunity to move towards cashless Indian society. According to data released recently by the Reserve Bank of India (RBI), the value of total transaction rose to $2 Tn (INR 131.95 Tn) in January 2019, making it the second highest reported in a single month over the last one year. (Dhananjay and Suresh Chandra, 2015) Even the government has taken initiatives to encourage people to do the transactions digitally. Indian government has introduced its own digital banking app called “BHIM”. For the Government also the digital transaction is beneficial for 2 reasons. Firstly, it is impossible to evade tax when transactions are done digitally as everything is recorded which is not the case in cash transactions. Secondly, it speeds up the overall sales which contributes proportionately to the growth of countries GDP.
1.3 Rationale of the topic

What is the issue?

India along with the other parts of the world has witnessed the rise of the alternative channel of banking along with the spike in cyber frauds. According to Reserve Bank of India a total of 2059 cases of cyber frauds amounting to 13.75 million euro were reported in 2017-18. The public sector banks have lost a total of 100 million euros in last three years. The banks are beefing up the security measures to tackle the proliferation of the cyber frauds along with a better redressal system for consumers (Frauds in Indian banking system, C. Singh, 2016). As a result of this, on one side the customers are losing confidence on the banking system and on the other side the capital of the banks are getting eroded which is very essential for the banks to comply with BASAL III norms.

1.4 Problem statement

It is clear that the cyber fraud is a big issue today which is on one hand making the consumers less confident on the banks and on the other hand it is creating a big dent on the profit of the banks. To eliminate this problem the banks are constantly enhancing their capabilities to fight against this fraud by adopting newer technologies like data mining, neural networks, machine learning, blockchain etc. Even Reserve bank of India has come forward to tackle the situation involving national security agencies like Central Bureau of Investigation and local police depending on the magnitude of fraud. (RBI Master circular, 2017) The main objective of these steps is to boost up the confidence level of the customers. If people loose trust in banks then following things will happen-

- Banks will lose the cheaper mode of funding as people will prefer to keep money somewhere else.
- People will stop using alternate channels of banking which will increase the operational cost of the banks.
- If banks loose CASA (current account/savings account) deposit because of lack of trust, then banks will not be able implement BASAL III for which increased amount of capital is needed as buffer against risk weighted assets.
- Indian government may have to intervene by funding via recapitalization to counter the problem of depleting deposit base.
1.5 Research aim

The aim of this research is to find out different types of cyber fraud, steps taken by the banks to counter this threat and to assess their impact on bank customer relationship.

1.6 Research objective

The objectives of the research are as followed:

- To identify the categories of electronic frauds take place in the Indian banking sector.
- To understand the effect of socio demographic factors of the customers on the electronic frauds in Indian banking system.
- To find out what steps the bank regulator has taken to counter the problem.
- To understand how the banks are addressing this issue.
- To understand how technology is being used to handle this issue.
- To understand the impact of electronic bank frauds on the consumer behaviour.
- To understand how these fraudulent activities can be minimized.

1.7 Research Question

Research question is the central question that a study is going to research about. All the investigations will be done based on the research question only. Therefore it is very important for the research to select a well-defined research question, which will serve as guideline for this research. Considering all these factors the following research question is carefully chosen:

'Is the technological innovation potent enough to reduce fraud, and increase trust, in the Indian banking system?'

The in-depth study regarding this topic will help the researcher to broaden his knowledge in the field of new types of electronic banking fraud, their prevention and their overall impact on the bank customer relation.

The researcher also aims to find the answers to the following questions:

a) What is the scale of the electronic banking fraud in India?
The research sought to find out the monetary value of the electronic fraud to understand the importance of the topic.

b) What are the new types of electronic frauds in the banking?

Changing banking habits have invited new techniques to make unauthorized electronic transactions. It is very important for the researcher to know about the new types of electronic frauds before trying to find out the solution for the same.

c) What are the Implications for the Indian banking system?

Indian banking system is already facing various issues now a days. Now this electronic fraud has added an extra headache for the entire banking system. The effect of this threat is not only limited to the banking industry but widely spread across the economy. The researcher tried to find out the direct and indirect impact of the same.

d) How the technological advancement is helpful in preventing the fraud?

Technology has stretched its helping hand to find a solution of this problem. It is also needed to mention that it is the technology which is creating new kinds of techniques to commit frauds.

e) How technology is being used in the Indian banking system?

The researcher tries to find out whether Indian banks are using the might of latest technology to prevent this threat. The researcher tries to find out the Reponses from the officers of scheduled commercial bank in India.

d) What is the impact of the fraud on bank customer relationship?

The electronic fraudulent activities are capable of stealing bank customer’s money. Certainly the customers look for alternative avenues to park their money. The banks are coming out with modern technological solution to fight against this. Sensing the seriousness of the matter, Indian banking regulator RBI has also stepped in. The researcher tries to find out the impact of the fraud on the customers by taking the responses of the industry people.
Chapter II

2. Literature review

The literature review will help in providing theoretical information regarding the topic. The recent studies regarding this topic will be discussed in this chapter. Newer techniques to commit fraud will be discussed here. How the banks are being effected and what are the steps they are taking with the help of technology to counter the threat will also be explained here.

2.1 Literature Review 1

Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures; (Dr. Sukhamaya Swain, Dr. Lalata K Pani, 2016)

This research shows different kinds of banking frauds taking place today across the banks like different types of atm frauds and technology related frauds. It explains how the frequency, complexity, and the money involved in the frauds have increased many times. The occurrence of these frauds has become a serious concern for Indian bank regulator like RBI. Banks have lost Rs 32000 crore (4 billion euro) because of the fraudulent activities last year. The amount is increasing every year. It demonstrates measures taken by RBI to prevent this kind of fraudulent activities.

In earlier times the types of bank frauds were very limited like fake currency circulation, forged security items like cheques, demand draft, pay order etc. Today the kind of fraudulent activities has changed because of the advancement of the technology. These activities have also fuelled because of the changing banking habits of the bank customers. Today bank customers do not like to visit retail branches for banking instead they prefer mobile banking, internet banking, online shopping for the same. This is the main reason behind the advent of newer techniques of cybercrime. Today around 70% of the total banking frauds are technology related frauds. These are committed by internet banking channel, ATMs and other payment channels like credit/debit/prepaid cards. The newer technological inventions offered by the banks have opened new opportunities for the cybercrimes. For an example the continued popularity of the web, mobile, cloud and social media have increased the prospects of the attackers. The trend of outsourcing, offshoring and third party contract to reduce the operation cost has also diluted the institutional control over the IT systems and access points. The new types of these kinds of frauds are:
1. **Hacking:** The hackers use to obtain unauthorized access to do transaction of any particular account. These kinds of frauds are not limited today to personal accounts. The banking system worldwide have created “SWIFT” (Society for Worldwide Interbank Financial Telecommunication code) platform to make secured interbank transactions (for import-export and international monetary transactions). The hackers had hacked even the credentials of the SWIFT from Bangladesh Bank and robbed $1 billion in 2016.

2. **Phishing:** This is a technique to obtain details of personal debit/credit card. The fraudsters send a fake mail asking some details to the bank customers which look like a mail send by the bank. The customer provides the details of the card and account in the mail which in turn gives the unauthorized access of the card to the fraudster.

3. **Pharming:** By this technique the fraudsters install malware in the personal computer to obtain details of the bank account / card without the knowledge or consent of the customer.

4. **Vishing:** Here the fraudsters use phone to obtain the information regarding bank account.

5. **Smishing:** It uses text messages to obtain the banking information of the customers.

6. **Debit card skimming:** In this method a chip look like card reader is installed in place of original card reader. Whenever customer inserts his/her ATM card this chip reads the number and pin of the card. The fraudster then gets the access of that card via that chip. This data could then possibly be reused to clone a magnetic stripe card.

![ATM diagram](image)

**Figure 2.1**

Newer kinds of risks have emerged with the advent of mobile banking in recent times. The possible frauds with mobile banking are:
1. **Fake apps:** In this process the hackers creates a fake apps which looks exactly like the original one. Once the customer installs the fake apps and provides information like password or pin, the fraudster gets the access of the account / card.

2. **Mobile banking application mapped to an incorrect mobile number:** This method is used for those customers who do not use the mobile banking. Here any bank employee can attach associates mobile number to the bank account and installs the mobile application on his own mobile instrument. Thus the details of the customer account is compromised by the associate keeping the customer in dark.

3. **SIM Swap:** The fraudster first collects the details of the account by phishing, vishing, smishing or any other method. Then they make the SIM card blocked and obtain a duplicate SIM from the mobile operator. It now becomes very easy for the fraudsters to do the transaction with the One Time Password (OTP).

**Preventive action:**

1. A fraud monitoring cell has been set up by Reserve Bank of India.

2. As per the new instruction by RBI, all the fraud monitoring and fraud investigation system is to be headed by the CEO of the bank.

3. The regulator has instructed the banks to disclose and make provisions for the fraud cases not exceeding four quarters from the date it has been detected.

4. Fraud reporting structure has been defined by the regulator.

5. Banks have to compensate the losses of the customers which have taken place not because of any fault by the customer.

### 2.2 Literature review 2

**Real time fraud detection in the banking sector using data mining techniques/algorithm (S.N. John et al 2016):**

The banks now a days are facing a big challenge of keeping customer’s account secure while avoiding complexity in login process. The customers dislike complicated passwords, hardware token devices and other out bound communication tools introduced as security measures by some financial institutions. It is a better idea to merge the security strength of an authentication
server with the logic of fraud detection system to identify suspicious behavior and step up authentication. On the other hand in case of normal transaction behavior to step down the authentication to minimize the inconvenience of the customer and making him satisfied.

Among several data mining methods classification, clustering, association, prediction and sequential patterns are used to detect the fraud. Classification is the widely used data mining technique that employs a set of pre classified example to classify the population of records. Clustering is a technique where population with similar behavior can be combined in a particular group. It can be used as preprocessing approach for attribute sub set selection and classification. For an example the demand for some brands in rural areas will be different from urban areas.

The main role of association rule is to find the set of variables that occur frequently in a transaction database. In association rule, if/then statements help to find out correlation between unrelated data. An example of an association rule can be “if a customer purchases bread then it is 90% likely to buy butter”. Prediction discovers relationship between dependent and independent variables. This technique is very much used to predict fraudulent transaction in the banking system. Money can be considered as independent variable where fraudster as dependent variable. Then on the basis of historical data fitted regression curve can be drawn which is used to detect online frauds. The sequential patterns analysis is used to identify identical patterns in data transaction over a period.

Banks are having existing record of each customer’s transaction history. Suppose it is noticed that a customer never transacts more than 500 euros from at once. This information acts as support in relation to association rule. So it can be concluded that if any request comes from the customer to withdraw above 500 euros the alarm will be raised which will prompt an additional authentication. It is having a very lesser probability that the fraudsters will know the customer’s transaction limit, though the credentials to make any electronic transaction are known to them. In an attempt to transact more than the transaction limit they will be faced with another authentication question. It will rarely happen that the fraudster will know the answer of that authentication question and the transaction will go through. To make the system stronger it is essential to create the answer of the authentication question case sensitive. An addition of special character will make this fraud detecting system even more effective.

2.3 Literature review 3

Two step prevention model of ATM fraud communications (Ossama H. Embarak, 2018)

In recent years ATM frauds have a new headache for the banks as newer methods like card skimming has become very common to make fraudulent transactions. Skimming happens when the fraudsters steal the electronic data which enables them to counterfeit the card and use it as
legitimate user. Card trapping is another method where victims ATM card is trapped in the machine by a device which is injected by the fraudster in the machine. Viruses and malwares are also used widely to violate the confidentiality and authenticity of the ATM transactions. By using ATM-malware method ATM PC is targeted and allows attackers to intercept card and pin at the ATM. This type of frauds represents almost 75% of the logical frauds.

Frudblock is a comprehensive solution to provide real time solution against frauds. This system accumulates historical transaction data to identify and prevent frauds. The system blocks fraudulent transactions by using parameterized rule based structures. Another system called Smartvista fraud prevention and monitoring system also uses historical data for fraud detection. They create a set of rules for the same which gets updated with fraud cases reported.

Non-physical attacks depend on the theft of user authentication data, malware, virus etc. in the card network back end infrastructure. If the standard path of the transaction is broken then even the fraudsters having the authentication data will not be able to complete the transaction. Attacks can be local or remote. In case of local attacks fraudsters use correct authentication data with counterfeit card. Remote attack happens during the transaction processing within the network as per the figure 1.

![Figure 2.2](image)

Algorithm is suggested as per figure 2 to counter the local and remote attacks. A bank base application should be installed on bank end system, ATM and user smart phone (GSTP).
Whenever a customer log into an ATM machine with correct PIN the system will start a transaction session in which the Back-end banking system (BES) will start operating and send one Transaction processing number (TPN) to the user’s registered mobile number as well as to the ATM. The user smart phone system (GSTP) configured to check if the smartphone physical ID is matched with its physical number. If no match found then GSTP will damage the received barcode. If match is found then the user will receive the TPN and transaction will be processed by entering the same. The main aim of using user’s smartphone device is that even if fraudster got legitimate user authentication PIN number, the fraudster would not be able to perform a transaction without users’ registered smartphone physical device, not the CIM number. Furthermore, if fraudster gains access to user’s smartphone device, he should not know the user's PIN number which should be used to begin a transaction. The only situation in which the fraudulent can complete the transaction when he has the user smartphone physical device, CIM card and user’s PIN number which is expected to be sporadic.
Figure 2.3
2.4 Literature Review 4

THE FIGHT AGAINST BANK FRAUDS: CURRENT SCENARIO AND FUTURE CHALLENGES: Dr Madan lal Bhasin (2016):

Banks are the growth engine for any economy. Banking industry is also growing very fast with the rapid growth of the economy. Indian banking system is expected to become third by 2025 according to KPMG. The number of frauds are also growing simultaneously with innovative techniques. Today there is no single bullet for protection against bank frauds. The newer application of neural network based behaviour models has changed the fraud management system around the globe. Banks, who are sitting on a pile of cash can afford to invest in technology and analytics for early detection of frauds which will eventually reduce the loss by the fraudulent transactions.

The other ways to control the frauds are:

1. Customer awareness about the fraud prevention.
2. More stringent application of laws
3. Using the might of data analysis technology.
4. Implementation of stronger fraud mitigation system
5. Following the multipoint scrutiny mechanism.

Indian bank regulator RBI has introduced Central Fraud Registry as a measure to counter frauds. Also it has instructed central investigating agencies sharing their databases with the banks.

It is seen that during last 50 years bank crisis and failure had taken place because of the fraudulent activities. So it is very important for the banks to get actively involved in protection of fraud to retain its customer base. The surge in usage of ATMs, internet banking, mobile banking is visible today. The fraudulent activities in the electronic channels are bringing not only losses to the bank but also effecting the credibility of the financial institution. Today data analysis software enables auditors and fraud examiners to enhance the security against fraudulent transactions. Banks have taken initiative in identifying suspicious transaction reporting, effective fraud risk management measures, whistle blowing processes to counter this threat. The key technical initiatives taken by the banks are:

1. Integration of fraud management system with IT security.

3. Consolidation of legacy system including cross financial crime prevention tool kit.


RBI, the regulator of the Indian banking system has instructed the banks to follow the following instructions:

1. Adoption of appropriate technology: A strong combination of authentication system and analytical software can reduce the threat of fraud significantly.

2. Stringent internal control

3. Screen job applicant carefully: Thorough background checking of potential candidates to be done. Banks should also consider drug testing and honesty testing.

4. Educate customers and employees.

5. Prosecute Thieves: Banks should show zero tolerance attitude towards any crime.

Early fraud detection has also become very important this time to reduce the fraud cases. Senior management and directors of the banks use to lead the fraud detection team. A range of approaches should be included in the fraud prevention system like point in time and recurring. The point in time testing will help to identify transactions which are to be investigated. If it comes out with any positive result then recurring testing should be conducted to come to a conclusion. Today, most of the banking process are based on technologies. This allows the fraudster to exploit the weakness to commit fraud. Internal audit should look at technology as an weapon to counter the threat. According to ACL the following analytical techniques can be very useful to combat the fraud:

1. Calculation of the statistical parameters to indicate the fraud.

2. Look out for patterns amongst elements of data and classify them.

3. Stratification of numbers to identify unusual entry.

4. Use of Benford’s law for identification unexpected occurrence of digits in naturally occurring data set.

6. Identify matching values in inappropriate places by joining diverse sources.

7. Identifying duplicate transactions like payments by duplicate testing.

8. Use of gap testing to find out missing value in sequential data.
RBI instructed the banks to follow up vigorously with CBI or police in any kind of fraudulent activities. All fraud cases below Rs. 1 crore to be reported to the local police. If the Central vigilance committee and CMD find any fraud serious then the same will be referred to Central Bureau of Investigation team. Cases above Rs. one crore has to be automatically referred to different wings of CBI depending on the nature of fraud. In case of private sector bank any fraud above 1 lakh is to be reported to the local police. Any response of fraud has to be quick sending a right message to the customer. The proper action of RBI involving local police, CBI, SFIO has resulted in curbing the fraudulent activities and helped in enhancing the confidence among customers.

### 2.5 Impact on customer behavior

The increasing online fraud in the financial sector has dampened the confidence of the customers on the banks. Almost 18% of the Indian bank customers had reported online fraud in 2018 which is more than any other country. Only 6% consumers in Germany and 8% in UK had reported electronic bank fraud. The fraud occurred across all ages but with different frequency depending on the age group. The most affected age group by this online fraud is 27-37 years. In this age group the usage of mobile banking application is the highest. Almost a quarter of the population of this age group had reported fraud. (FIS report, 2018)

The bank fraud directly discourages banking habit of the people. They become skeptical about the safety of their hard earned money. Customers experience considerable time and emotional losses when such fraud happens without any fault at their end. This may develop a perception of the customers towards banks that their asset is unsafe with the bank (Barker, D’Amato and Sheridon, 2008). This may lead the customer to choose alternative avenues to park their money.

Earlier the banks used to take too long time to compensate the loss as there was no specific guideline for the refund. This is because at the time of making any digital transaction, it goes through various intermediary platforms like payer bank, payee bank, payment gateway etc. Also the transaction use to be encrypted. No data is to be stored but to be transferred (Hoffmann and Birnbrich, 2012). So in case of any fraud customer cannot be held liable. For an example some banks like ICICI, SBI, YES bank had outsourced “Hitachi Payment Service” who has compromised ATM transaction data of 3.2 million cards which had resulted in many frauds. In this scenario RBI has stepped in to boost customer confidence and came out with a guideline in 2017 stating that if the customer intimates the banks regarding fraudulent transaction within 3 working days, the bank will have to compensate the entire monetary loss to the customer.(Business Today, 2017)
2.6 Alternative avenues for the consumers

2.6.1 **Stock market:** Indian stock market has given a return of 20% return at a compounded annual growth rate (CAGR) in last 20 years. This figure is way above than US and Chinese stock market index. So stock market is a good alternative for the consumers to park their funds. (Bloomberg, BOFA Merrill Lynch Global research, 2017)

![Proportion of current indices that have delivered 20/15% CAGR returns over 20yrs](image)

**Figure 2.4**

2.6.2 **Mutual Fund:** Equity mutual funds as well as debt mutual funds are also good avenues for the consumers to park their funds. From the graph below it is easily understood that the growth in mutual fund asset (AUM- Asset Under Management) has grown the fastest when compared to the rest of the world (IIFA report, 2018). The main reason behind this is the strong performance of the Indian equity market over the years. Also the default risk is quiet low in certificate of deposits and commercial papers issued by Indian corporates, which in turn made the debt mutual funds increasingly popular among Indians.
In the below figure it can be seen that every year the consumers are moving away from the banks slowly but steadily towards mutual funds in terms of investments.
2.6.3 Gold: Gold is a financial instrument which is universally known as “inflation hedge” (Dipak ghosh, 2001). The gold price was examined against consumer price index (CPI) by the autoregressive distributed lag model (ARDL) which shows that it is really an effective tool against inflation (Mohammed Hassan Shakil et al, 2017).
Figure 2.8  

Source:  www.ibjarates.com

Figure shows that gold is not only an inflation hedge but a good avenue for investment also as its return has surpassed stock market return in the long run.

### 2.7 Implication on the banking system

The loss of confidence of the customers can affect adversely towards bank because of the following reasons:
a. **Banks will lose the cheaper mode of funding as people will prefer to keep money somewhere else:** A bank first collects low cost deposits from its customers. Then it lends to the industries, individuals at much higher rate. The difference between two is known as Net interest income which is the main component of the bank’s operational profit.

In India banks provide interest @ 4-5% against funds kept in the savings bank. Whereas banks do not pay any interest against the fund kept in the current account. These are the sources of cheapest deposits available in the Indian financial system collectively known as “Demand liability”. With these deposits banks use to lend to the individuals (home loans @ 8.5-9.5%, personal loans 15-17%), industries (@ 12-14%), farmers (9-10%).

![Table: MCLR Rates of Select Banks](image)

<table>
<thead>
<tr>
<th>Bank</th>
<th>Old base</th>
<th>MCLR overnight</th>
<th>One mth</th>
<th>3 mth</th>
<th>6 mth</th>
<th>1 yr</th>
<th>2 yr</th>
<th>3 yr</th>
</tr>
</thead>
<tbody>
<tr>
<td>BoB</td>
<td>9.65</td>
<td>9.00</td>
<td>9.00</td>
<td>9.05</td>
<td>9.10</td>
<td>9.30</td>
<td>-</td>
<td>9.35</td>
</tr>
<tr>
<td>Canara</td>
<td>9.65</td>
<td>9.00</td>
<td>9.25</td>
<td>9.35</td>
<td>9.40</td>
<td>9.45</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ICICI</td>
<td>9.35</td>
<td>9.00</td>
<td>9.00</td>
<td>9.10</td>
<td>9.15</td>
<td>9.20</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

MCLR: Marginal cost of funds-based lending rate (w.e.f. April 1). It is a tenor-linked benchmark. Sources: Bank statements, releases.

So it can be said that if customers stops keeping money with banks due to the fear of fraud, banks will not be able to fund the industries or individuals for any kind of requirement of loans.

b. **Decrease in credit growth:** Industries run on bank credits which generates direct and indirect employment creating demand for goods and services and impacting GDP growth. So it is very important for the banks to be a secured place to park the funds in the eyes of the consumers. (Charan Singh, 2016)
We are already witnessing a slowdown in credit growth for various economic reasons. At such difficult time our banks can not afford to lose customer base because of the fraudulent activities.

c. **Basal III**: Basal III regulation was developed by bank of international settlements to enhance the stability of the bank in case of economic downturn. As per this regulation, banks have to keep higher amount of capital (4.5%) as buffer against risk weighted assets (RWA). (BIS report 2017) Reserve Bank of India has decided to implement Basal III from 2020 in the overall banking system.

So it is very clear that banks need additional capital for Basal III. This additional capital will come in the form of increasing deposits. If consumers start losing confidence in banks and starts withdrawing money then the banks will either fail to comply with Basal III or will have to ask the government for recapitalization.

### 2.8 Latest methods to commit frauds

#### 2.8.1 Black box attack: In this method the cybercriminals gets the physical access of the ATM top cabinet where the ATM PC core is situated and then puts the ATM in supervisor mode. Then the ATM network cable is removed so that the ATM cannot be monitored. The attacker then installs malware (Black box) in the ATM PC to control the cash dispenser. The blackbox can be controlled by a smartphone to give instructions for dispensing cash. For the customer it is still in supervisory mode whereas ATM dispenser is still working. With the smart phone the attackers give command to dispense cash till it runs out of money. After the theft the attackers remove the blackbox from the device, leaving no traces. (Enisa report, 2018)

#### 2.8.2 Man in the middle attack: In this kind of attack, bank’s internal network infrastructure is compromised and the network traffic is monitored by malware. When the malware intercepts any cash withdrawal message, it alters the host response from ATM switch and changes the authorized dispense amount to a larger sum. The attacker will then use the predefined card to withdraw the money at any ATM on the compromised bank network. The transaction will be intercepted as the card number will be recognized by the malware. As the malware has already altered the amount of cash to be dispensed in the response from the host, the ATM will dispense more cash what is debited from the account. (Avijit Mallik, Abid Ahsan, Jia Chi Tsou, 2019)

#### 2.8.3 Ransomeware attacks: The world has seen the devastating impact of a malware called “Wannacry” in many organisations. It encrypts files on end points those which are running Microsoft operating system. The files are decrypted only on the payment of ransom money
demanded by the attackers. There are some ATMs in India which are attacked by this malware. (Ella Nsonta Kasanda, Jackson Phiri, 2017)

2.9 Latest technology to prevent fraud

2.9.1 Blockchain technology: A Blockchain is a digital, immutable, distributed ledger that chronologically records transactions in near real time. The prerequisite for each subsequent transaction to be added to the ledger is the respective consensus of the network participants (called nodes), thereby creating a continuous mechanism of control regarding manipulation, errors, frauds and data quality. Digital ledger of transactions is created which shared among network of computers. It also maintains continuously increasing list of records called “Blocks” which are immune from tampering. The prime advantage is that it uses cryptography which allows different users to modify the transactions on a secured network each one accessing their node of data. If majority of nodes agree that the transaction performed looks valid, identifying information which matches the blockchain’s history and thus a new block is added to the chain (Tejal shah, Shailak Jani, 2018).
Once a block of data is recorded on the ledger then it is very difficult to alter or remove it. If anyone wants to add anything, the miners who are the participants in the network verify the proposed transaction. As the blockchain works as a ledger or database which can store all types of information exchange which is accessible to every participant of the network. As the every transaction in the blockchain is checked by independent miners, there is a realtime analysis and verification done at every step. For this reason it is very difficult to commit fraud in a blockchain system (Tejal shah, Shailak Jani, 2018).

In 2013 hackers deployed a malware through email in Bangalaesh Central Bank and got access the credentials to operate “SWIFT”, by which they had stolen $100 million from the bank. In these kind of case blockchain technology could have been useful as it would create a compete record of transactions which would be held in on multiple computers effectively preventing the record being altered. Moreover 8000 members of “SWIFT” would have seen the message in the blockchain based “SWIFT”, reducing the chances of any fraudulent message go through. Some people blame the outdated single signature method of the payment system. Blockchain technology based Ripple Consensus Ledger (RCL) is multi-signing which increases the security of the network.(Shailak Jani, 2018) In 2018 Nirav Modi had committed a fraud of almost 1400 million euros by the way of issuing fake letter of undertaking via “SWIFT” which were not recorded in the internal system, from a state owned bank called Punjab National Bank. Here also it is suggested that blockchain technology would have prevented this fraud. Blockchain would have blocked the transaction as the “smart contract” feature would have identified
inconsistencies based on automatic reconciliation with core banking system and payment
initiation would have been restricted over “SWIFT” network.

2.9.2 Neural Network: This is also being extensively used today as tool for fighting against
frauds. This system works on the basis of the knowledge of previous cases of frauds and gets
updated continuously. Fraud cases are statistically analysed to derive out relationships among
input data and values for certain key parameters in order to understand the various patterns of
fraud. With this knowledge the system becomes able to identify similar fraud cases in future
(Madan Lal Bhasin, 2017).

Today most of the studies regarding prevention of credit card fraud, are getting carried out by
neural network. In” CARDWATCH” system the neural network is trained with past data of a
particular customer regarding spending behaviour to detect possible anomalies. Falcon,
developed by HNC, uses feed-forward Artificial Neural Networks trained on a variant of a back-
propagation training algorithm. Machine learning, adaptive pattern recognition, neural networks,
and statistical modeling are employed to develop Falcon predictive models to provide a measure
of certainty about whether a particular transaction is fraudulent. A neural MLP based classifier is
also works on the principle of neural network. It acts only on the information of the operation
itself and of its immediate previous history, but not on historic databases of Author's personal
copy World Wide Web past cardholder activities. (Wei Wei· Jinjiu Li·Longbing Cao, 2012)

2.9.3 Artificial intelligence: Today artificial intelligence is being used to detect financial
frauds by using in the IOT (Internet of Things) environment. Fission computing is very much
used today which relies on edge-crowd integration for maintenance of security in the IOT
environment. Another efficient fraud detection system which is adaptive to the behaviour
changes by combining clustering techniques is composed of two stages. In the first stage it
compares the incoming transactions against the transaction history to identify anomaly using
BOAT algorithm. Whether the suspected anomalies are due to the fraudulent transactions or any
short term changes in the spending behaviour in the second stage is analyzed. A machine
learning based research has also been proposed as a web service based collaborative scheme for
credit card fraud detection. Dempster-Shafer adder (DSA) based on Dempster-Shafer theory and
Bayesian learning research is also proposed to detect financial frauds. In this method, a
transaction with suspicion score can be referred to as highly probable fraudulent transaction
based on the index in the transaction history database. BLAST and SSAHA algorithm are used as
sequence algorithm to efficiently examine spending behaviour of the customers. Hidden Markov
Model (HMM) is also proposed to detect frauds by building multilayer model of programs.
Genetic algorithm is used in finding frauds in real time (like- credit card frauds) and to minimize
the false alarm. Decision trees and support vector machine are supervised learning methods which detect normal and fraud transactions by classifier (Dahee Coi, Kyunghu Lee, 2018).

2.10 Application of technology in Indian banking system

The Indian banking sector is in a process to implement a blockchain based platform with SWIFT India and Monetago to secure all the trade finance related transactions. Earlier Monetago had developed blockchain based platform called Trade receivable discounting system (TReDS) to prevent double financing of invoices. Till now SWIFT has partnered with 34 international banks including Deutsche Bank, Commerz Bank, Jp Morgan chase bank to create a blockchain platform for nostro accounts. Nostro accounts are accounts held by a domestic bank on behalf of a foreign bank, to facilitate trade financing and other cross-border transactions. Blockchain technology through its distributed ledger technology enables banks to monitor real time liquidity, easy reconciliation, transaction status update which in turn helps to keep the transactions safe. It is also argued that $100 mn fraud in Bangladesh central bank could have been prevented in the presence this system (American express, 2018).

Another private sector bank called Kotak Mahindra bank partnered with Deloitte to implement blockchain based end to end trade finance system to secure Letter of Credit transactions. Kotak bank is also exploring the possibilities to implement blockchain technology in cross border transaction, user identity management, trade settlements (Economic Times, 2017). This bank has upgraded its ATMs to eliminate XP based system for better virus and malware protection. They also have come out with new system to mitigate the risk of APT (Advanced Persistent Threat) (Kotak Mahindra Bank annual report, 2019). HDFC bank follows effective framework to manage cyber security which is based on 4 pillars- protect, detect, respond and recover. They also have deployed a committee of board which dedicatedly looks into cyber security issues. The bank has also updated Security Incident and Event Management (SIEM) to enhance security of IT infrastructure. It has also deployed Deception Technology Solution to detect, analyze, defend real time advanced cyber threats. HDFC Bank has also updated firewalls to next generation with Deep Packet Inspection (DPI) ability which analyzes packets of information transmitted across the web. This has enhanced the protection against malwares, ransomwares in the banking channel. Risk engine and transaction monitoring system monitor the suspicious transactions on internet banking, ATM and e commerce channels. It has also upgraded the anti-phishing system which detects and shuts down the phishing sites more effectively. The bank has PCI DSS 3.0 certification which confirms that the ATM/credit/debit card holders of the bank enjoy a high level of safety from frauds (HDFC Bank annual report, 2019). On the other hand another private sector bank Axis Bank adopted a holistic cyber security program with comprehensive cyber security policy (CSP). It has designed its cyber security framework based on National Institute of
Standards and Technology (NIST) standard which is also compliant to ISO27001 standard. The bank has also enhanced web security by deploying the followings: 1. Web site anti phishing monitoring solution, 2. E mail anti-spamming and anti-phishing solution, dark web deep insight monitoring capabilities, cloud security framework (Axis bank annual report, 2019). The largest bank of India, State bank of India has implemented Network Access Control (NAC) for protection from cyber attacks by preventing the access to the network by unauthorized and non-compliant endpoints or devices. It has made its branches subject to IS audits to assess the IT related risk periodically (State Bank of India annual report, 2019).
Chapter III

3 Research Methodology

The most important of any research is the data and methodology. In this dissertation, the choice of data and methodology is carefully chosen to avoid any criticism in this regard. The main purpose of this research is to find out whether the technological innovations are enough to build trust with the customers for the Indian banks. The research sought to investigate the effectiveness of the new technological advancement in the field of cyber security. In this chapter the researcher will incorporate various concepts, theories and ideas by following a structured research method. Here the researcher would gather information from the best possible respondents which in turn will be beneficial to conduct the research in the best possible manner. The researcher collects the data analyze the same with research analytical tool to come to a proper conclusion (Green, 2011). At first the researcher has made a clear understanding about the topic by reading articles related to the research topic. Then a questionnaire is prepared to get the best possible responses from the respondents, to find an answer to the research problem. Data collection method was also chosen in accordance to the research problem.

3.1 Proposed methodology

Somekh and Lewin (2005) defined research methodology as collection of proper rules to carry out by which a particular piece of research is undertaken. This part provides the information regarding the methodology which is an important part and parcel of the research.

3.2 Research design

The research will be conducted by following the ‘research onion’ model presented by Saunders et al. (2009). Several layers can be found in that ‘research onion’. The layers to be peeled one by one starting from the outer most layer, to reach the core part of the research process.
3.2.1 Research Philosophy

Philosophy of the research can be found at the outer most layer regarding which Saunders et al. (2009, p.108) opines that it contains important assumptions which will be helpful to choose the correct research strategy and method.

Subjectivism

The research will follow the philosophy of subjectivism to understand the effect of technological advancement to prevent electronic frauds on bank customer relationship. Subjectivity guides everything from the choice of topic that one studies, to formulating hypotheses, to selecting methodologies, and interpreting data. In this research, the researcher tried to reflect on the values and objectives which he brought to the research and also tried to find out their effect on the research. Subjectivity can bias the researcher and preclude objectively understanding a subject's psychological reality. However, this is not inevitable. In fact, one of the advantages of
recognizing subjectivity is to reflect on whether it facilitates or impedes objective comprehension. Distorting values can then be replaced by values that enhance objectivity.

The reason behind choosing the subjectivist philosophy is because the ever changing nature of banking and frauds. Today the way people bank is different when compared to banking habit used to have 20 years earlier. According to the change in the banking habits, the nature of fraud has also changed with the course of time. In other words the bank customer relationship is not constant because of frauds. It changes with the types of fraud and the counter action taken by the bank and the regulator.

**Interpretivism**

The followers of interpretivism rely on the fact that reality is multiple, relative and ever changing (Hudson and Ozanne, 1988). The knowledge gained by this method is socially constructed rather than objectively determined and perceived (Hirschman, 1985, Berger and Luckman, 1967, p. 3: in Hudson and Ozanne, 1988). Interpretivists do not believe in rigid structural framework and adopt a research structure which is more personal and flexible (Carson et al., 2001) and make sense of what is perceived as reality (Carson et al., 2001). The interpretivist researcher enters the field with some sort of prior insight of the research context but assumes that this is insufficient in developing a fixed research design due to complex, multiple and unpredictable nature of what is perceived as reality (Hudson and Ozanne, 1988). The researcher develops new knowledge during the study and remains open for the same throughout the study.

In this research the individuals have their own consciousness and give rational responses as they are the part of practical banking industry. They are not mere puppets who react to external social forces as positivists believe.

**3.2.2 Research approach**

The type of research approach is the next layer of the research onion. Normally there are two types of research approaches namely inductive and deductive research.

**Deductive approach**

This approach starts with a development of theory and hypothesis which is then tested by the way of observations to approve or disapprove the theory. Saunders et al. (2007) figured out the following main stages that define this particular approach: deducing a hypothesis from a theory, illustrating about how the hypothesis will be measured, hypothesis testing, examination of the result and modifying the theory if needed. This approach can be considered as a process with a general view at the beginning and which gets specific in the end.

**Inductive approach**
This approach begins with observations which are proposed at the end of research as a result of observation. Inductive approach comprises of the advancement of theory as an aftereffect of the perception of experimental information (Saunders et al., 2007). The main objective of this approach to allow significant themes of the raw data without any intervention of structured methodologies. The qualitative technique generally follows the inductive approach.

In this research the researcher followed the inductive research methodology as the research involved process of qualitative data collection and creates theory form the information obtained from the investigation. Inductive methodology gives a practical understanding of the issue (Saunders et al. 2007). The questions those are asked in the research starts with “What”, “How”, “Does” etc. to understand the ground reality of the issue for which the inductive methodology is more suitable in this case. One more reason to follow this approach was that the main purpose of this research was to move individual perception to explanation of general patterns. (Collis and Hussey, 2009).

### 3.2.3 Research Strategy

The next level of the research onion is the research strategy. Every sort of examination methodology could be utilized for each of the three purposes: exploratory, descriptive and explanatory (Yin, 2003). Collis and Hussey (2003) opines that there are many research strategies available to follow like grounded theory, ethnography, participative enquiry, case studies, surveys, longitudinal studies etc.

In this research to find out “the potential of technological innovation to reduce fraud and increase trust in the Indian banking system”, the researcher had followed the case studies and grounded theory strategies. The case study strategy has the potential to find out the answers to the questions starting with “why”, “what”, “how”. That is the reason why case study strategy is used for illustrative and exploratory examinations. So case study is the most suitable strategy to find out the answers starting with “what”, “why” regarding the innovations of technology to prevent fraud in the banking industry.

In this research, semi structured interview was conducted. The answers obtained from these questions enabled the researcher to find out the answer of the research question.

### 3.2.4 Research Choice

The very next layer of the research onion is the research choice which is of two types – qualitative research and quantitative research.
Qualitative Research

Qualitative research is a type of scientific research that have the following features:

- Seeks answer to any question
- Evidence collection
- Predefined set of procedures are used to find the answer
- Procedure findings are not determined in advance.

Also it tries to understand the research problem from the population it involves. This kind of research is specifically good to obtain information about behavior, opinion, value of particular population. The main advantage of qualitative research is to provide textual description regarding how people experience regarding a given research problem. This method is also useful in identifying intangible factors like the demographic profile and socioeconomic status of the participants.

Quantitative Research

This particular method can be defined as a kind of investigation to find out the answer of the research problem by gathering quantifiable data and performing computational technique. Information can be gathered by using online surveys, online polls etc. the result of which can be can be depicted in the form of numerical. This kind of research is mostly conducted in social sciences where statistical method is used to collect quantitave data. Mathematical frameworks and theories are deployed by the researcher in this method.

In this research the researcher will use qualitative method of research. Being a case study kind of research, the researcher will follow single data collection method. For the purpose of seeking qualitative information, in-depth interviews will be conducted.

Five in depth interviews were conducted in this research with five different bank officials who are manager or above manager level in rank. It was tried to take a wholesome view of the Indian banking system as interviews were taken with officials of one of the smallest scheduled bank (Cosmos bank), largest public sector bank (State bank of India), largest private sector bank (Icici Bank), medium sized public sector bank (Union bank of India) and medium sized private sector bank (Yes Bank). In-depth interviews are most suitable for circumstances in which one needs to ask open-finished inquiries that evoke profundity of data from moderately few individuals. (Guion L, Diehl D, and McDonald D, 2011).

3.2.5 Time Horizon

The very next layer of the research onion includes time horizon of the research. cross-sectional studies and longitudinal studies are the two types of time horizons. Longitudinal studies includes
researches which goes on a longer time frame and is commonly required in measuring change amidst this time period which is not suited to ventures with fleeting time confinements while cross-sectional studies are noted as previews of a specific phenomenon at a specific time (Saunders et al, 2007).

As in this particular research the time was limited, so this research selected cross sectional study. A cross-sectional study draws in the collecting data on more than one case at one particular time with a specific end goal to gather quantitative or quantifiable information when more than one variable is viewed as (Bryman and Bell, 2003).

3.2.6 Data Collection Method

This particular research is investigative in nature because of which qualitative method was followed. Also the use of non-numerical research technique in this research to find a proper answer to the research question, is also reason to choose the qualitative method rather than quantitative one. "Qualitative method is utilized dominantly as an equivalent word for any data collection technique, (for example, interviews) or data analysis procedure,(for example, classifying information) that produces or uses non-numerical information." (Saunders, Lewis and Thornhill, 2007)

Two types of data collection methods are there like primary data collection and secondary data collection.

Primary Data Collection

This the new data which is gathered by conducting interviews. Also it minimizes the chances of occurring any error during the research.

The main objective of the research is to find out the “potential of technological innovation to reduce banking fraud and increase customer trust in India”. The primary data was collected by conducting interviews with bank officials who are having vast experience in different verticals of banking. The interviews were taken via telephonic conversation.

The following questions were asked during the interview:

1. Has your bank been impacted by the cyber fraud?
2. What are the primary sources/causes of cyber fraud?
3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

5. What kinds of new/emerging cyber threats is your bank is experiencing?

6. What kind of risk polices your bank has implemented to address the cyber security?

7. How much your bank is spending on the research of cyber security?

8. How would you frame the relationship between fraud, trust and the future of commercial banking?

The interviews was conducted with manager of Cosmos bank, chief manager of State bank of India, location head of yes bank, senior manager Union bank, manager of Icici bank.

Secondary data

This type of data is available in the public domain. This was collected from previous articles, journals, books, websites regarding online banking fraud and prevention techniques.

3.2.7 Sampling

According to Mason (2002) "Sampling and selection are standards and techniques utilized to recognize, pick, and access to data sources". It is impossible for the researcher to collect data from whole population for which he has to choose a sample with specific data collection technique.

As per Field (2005) A Sample is "a littler gathering of units from a population utilized to decide truth/facts about that population". There are two types of sampling method one is probability sampling and another one is non probability sampling. The probability sampling generally used in methodologies where survey is used. The second sample technique is non-probability or judgmental sampling gives a scope of option strategies to choose tests in light of researcher subjective judgment.

As qualitative technique is used in this particular research, therefore the non probability sampling is used here. The size of the banking industry is huge in India and it is impossible to take a view from every personnel from every organization of this sector. Also the time and budget was limited because of which neither the samples were randomly selected nor they were randomly distributed.
3.2.8 Research Ethics

As the researcher plans to proceed with the research, concerns regarding ethics were raised. Cooper and Schindler (2008) describes ethics as the “standards or gauges of conduct that guide moral decisions about our conduct and our association with others.” The moral parameters of the association whose managers or authorities had participated. The interviewees were well informed regarding the topic of the research. The interviewees were given freedom of not disclosing their names. The Data Protection Acts (1988, 203) had been entirely taken after with the preparing and storage of data.

3.3 Research limitation

The very first thing before starting the research was to identify the limitations of the research and to decrease them to minimum. The most challenging part in this research was time management. As the interviewees were bank managers, so it was very difficult to get their free time. So to minimize this problem, the researcher had tried to fix the meeting at the initial stage of the research. The interviewees may not disclose some of the facts and figures as those information can be confidential to the organization.

In this research it was not possible to take face to face interviews, as the interviewer and the interviewee are in different countries. So the interviews were conducted via telephone. The body language of the interviewee could not been observed during the interview process.
Chapter IV

4. Data analysis

The analysis and findings of the research based on the interviews conducted with 5 bank officials who have vast experience in the field of banking, will be discussed in this section. The response of the participants were scanned to find out the answer of the research questions.

4.1 Methodology of research

In depth interviews were conducted with 5 bank officials who are having vast experience in schedule commercial bank in India. All the bank officials have significant IT experience also as to find out the research question one needs the knowledge of IT and banking. The interviewees are having overall knowledge of the banking system as they all have worked in retail banking, treasury, corporate banking etc. The researcher had tried to take the responses from the officials of the largest public sector bank (State bank of India), largest private sector bank (ICICI Bank) and from one of the smallest scheduled commercial bank (Cosmos Bank) to understand the overall situation in the banking industry. It is very important to gather the information from these different types of sources to realize how the overall banking system is utilizing the technological might to prevent the threat.

Three of the five interviews were conducted via telephone. Each interviewee had been given the form which explains the objective of the research. The questions were open ended which gives the interviewees express their own views freely. All the interviewees were asked the same set of questions to make the researcher able to find out the answer to the research question.

4.2 Participants Information

a. Participants Gender

All of the five participants were male.

b. Participant details

The details of the participants who were interviewed during the research is given below:
• Participant position: Manager (IT)
  Work experience in banking industry: 6 years.
  Name of the Bank: Cosmos Bank
  Country: India

• Participant Position: Chief Manager
  Work experience in banking industry: 12 years
  Name of the bank: State Bank of India
  Country: India

• Participant Position: Location Head (Mumbai Zone)
  Work experience in banking industry: 14 years
  Name of the bank: Yes Bank
  Country: India

• Participant Position: Senior Manager
  Work experience in banking industry: 10 years
  Name of the bank: Union Bank
  Country: India

• Participant Position: Manager (Branch banking)
  Work experience in banking industry: 8 years
  Name of the bank: ICICI Bank
  Country: India

4.3 Interviews

Five interviews were conducted during the research. All of the interviewees are posted at managerial level or above in scheduled commercial bank in India. The main objective of this research is to find out whether the technological advancement is able to enhance the trust among the customers on the banks. All the five interviewees work in different banks and have knowledge of wholesome banking as they have the experience of working in different verticals of banking like- retail banking, treasury, trade finance, corporate banking, SME banking etc.
1. Has your bank been impacted by the cyber fraud?

According to the manager of Cosmos Bank, yes their bank is heavily impacted by cybercrime. In the fiscal year 2018 they had faced an incidence of cyber fraud in which Rs. 95 crores was theft from Cosmos bank. It was a very big hit as Cosmos bank is a very small bank with deposit base of only Rs. 15000 crores. Apart from this incidence customers have reported almost 100 online fraud cases of which most of the transactions were below Rs. 1 Lakh.

As per the chief manager of State Bank of India also, his bank is also impacted by the cyber fraud. In 2016 State bank of India had encountered a massive cyber-attack in which malware induced security breach for which information about almost 0.6 million debit cards was leaked. Immediate action was taken by blocking the debit cards and re-issuing them. Also his bank is facing issues with card cloning, card skimming etc.

One of the private sector bank Yes bank is also impacted by the cyber fraud, according to one of the location heads of Yes Bank. In the fiscal year 2016 Yes bank had faced a major data breach of 3.2 million ATM card holders from POS (point of sale) terminals and ATMs which were managed by Hitachi payment services limited. The financial loss was restricted by blocking those infected cards and reissuing them. Apart from that incident, the bank is facing cyber-attacks like card skimming, card cloning etc. In the last financial yea , The bank had received almost 800 cases regarding fraudulent transactions by ATM cards.

One of the senior managers of Union bank of India also opines that his bank is also impacted by the cyber-attack. In 2016 union bank of India had encountered a major cyber-attack which was intended to steal $171 million by the hackers. It was one of the biggest online fraud in the Indian banking industry. This year Union bank of India had reported almost 50 cases of ATM frauds in the last financial year. In most of the cases card skimmers were used to do the fraudulent transactions.

India’s largest private sector bank, ICICI bank is also adversely impacted by cyber fraud, according to one of the branch managers. ICICI bank is most affected by the application of skimmers in the ATM machines according to him. In the last year almost 120 cases of were reported where money was stolen from ATM as the ATM skimmer was attached to the ATM machine. He also added that phishing mail is a big issue for our bank.

2. What are the primary sources/causes of cyber fraud?

According to the manager of Cosmos Bank, the technological advancement is mainly responsible for newer ways to commit cyber fraud. Also he had mentioned that may be countries like North Korea is becoming the main source from where these online frauds are getting organized. The
major cyber attack of 94 crore that cosmos bank had faced, was organized in North Korea. The culprits behind the Bangladesh cyber fraud also organized their crime from the same country.

As per the chief manager of State Bank of India, one of the primary sources of the cyber fraud is “Google play” app where fake banking apps are present in numbers. Once customers install the fake app in their mobile, all the personal data of the customer gets compromised with the fraudster. He also added that it is very difficult to identify these fake apps as they are very close copy of the original one. Sometimes they mimic the exact graphic design of the original app. Another reason he pointed out is the awareness among the customers. They sometimes do not take the proper measures to keep the personal data confidential and the same gets compromised with the fraudsters.

The location head of Yes Bank told that the ATM and POS (Point of Sales) of yes bank are managed by third party agencies (like Hitachi payment services) and there are always chances of data breach from their end as it happened in 2016. Another main source is the fake apps of Yes bank available in “Google play store”. Customer installs the fake apps and falls prey to the fraudsters. He also blamed the rapid advancement of technology is responsible for the same.

One of the senior managers of Union bank of India blames the changing banking habit of people for the cyber fraud. Today customers like online and mobile banking instead of going to branches physically. This transformation has taken place without proper knowledge of taking precautions. The fraudsters exploit this loophole and become successful in their intension of stealing money. He also added the advancement of technology for this threat. Because of newer types of malwares, it has become very difficult for any bank to detect and prevent them from infecting the system.

The branch manager of Icici bank had pointed out the fake apps available at google play store as the main source of the cyber fraud. These fake apps use to appear same as the original bank app. Customers erroneously download the fake app and start transacting with the same. Thus the confidential banking data gets compromised with the fraudsters. He also opines that customer awareness is also a reason why people lose money because of the cyber frauds. Today people of all age group and gender use the alternative channels like ATM, online banking. But many of them still not follow the safeguards because of their age, gender, educational qualification etc. which give the fraudsters the chance to steal money fraudulently.
3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

All the participants have told that their banks follow the guidelines given by Reserve Bank of India. If the online fraud is reported within three working days to the bank, then the customer’s liability is zero and the money is credited within 10 days to the customer’s account by our bank. If the fraud is reported after 3 working days but within 7 working days, then the liability of the customer is Rs. 25000/- maximum depending on the type of the account. If the same is reported after 7 working days, then the liability of the customer is fixed by the internal policy of the bank.

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

While answering this question the officials have told that their banks have taken different steps. Like cosmos bank has provisioned Rs. 18 Crore (2.25 million euro) for the cyber fraud. The state bank has taken an insurance policy covering $100 million to counter this threat. Union bank of India has taken a cyber liability insurance policy of Rs. 325 Crore (40 million euro). Whereas private players like ICICI bank and Yes bank have neither taken any insurance policy nor have provisioned any money in their balance sheet.

5. What kinds of new/emerging cyber threats your bank is experiencing?

The manager of Cosmos bank pointed out a new kind of threat in which the malware attacks the ATM switch and makes it malicious. The attackers first enter into the network by sending spear phishing mail. Once malware was inserted into the system, it sets up ATM/POS proxy switch which is in parallel with bank’s own central switch. The connection between the core banking system and bank’s central switch is then redirected because of which the required messages to authorize debit card withdrawals never get forwarded to the core banking system. So the card number, pin etc. could not have been checked by the core banking system. On the other hand fraudulent messages are sent from the malicious switch to authorize fraudulent transaction. Many of the ATM cards get cloned and money gets withdrawn from various ATMs in different countries. This type of attack in which a proxy switch was generated by inserting a malware, is new to the Cosmos Bank according to him. Eventually the same bank had lost Rs. 95 Crore because of this malware.

According to the chief manager of State bank of India, they are experiencing a new type of attack called DDOS (Distributed Denial of Service) where the malicious traffic restricts the genuine
traffic to go through to original application. Once this attack becomes successful in penetrating the firewall, it infects the core banking system.

The location head of Yes bank had informed us about a new kind of malware specially designed to attack “SWIFT” terminals which is sent by a malicious mail. After the Bangladesh bank heist, the attackers have turned their focus on “SWIFT” terminals as high value cross border transactions take place via “SWIFT”. New types of malwares which target the components of the internal IT infrastructure of the bank like operating system, databases, files, firewalls etc. are also newer threat to the bank. These malwares are getting technologically advanced day by day as per him.

The senior manager of Union bank of India has also added the threat of attack at their SWIFT terminals are the emerging threat to his bank. Union bank of India has already experienced a cyber attack which was attempted to steal $171 million in 2016. At first a malicious email containing the malware as attachment, was sent from an authentic source – RBI (Reserve bank of India) to many of the employees. The attachment was in a zip file which was dot (xer) file instead of dot (pdf) file. As soon as one of the employees opened up the email, the malware got released in the system and the fraudsters got access of credentials of the SWIFT. By login into SWIFT account the hackers had been able to send $171 million to the banks in Cambodia, Thailand and Australia which was routed through Citibank New York and JP Morgan Chase New York. They had also tampered with SWIFT’s prt file where they had deleted those 6 entries of the fraudulent transactions. When the very next day the SWIFT transaction report came and reconciled, it was found that $171 million was stolen from the dollar nostro account. Immediately the money trail was traced and the transaction was blocked. Thus our bank did not incur any lose because of this attack.

The modus operandi of the attack was same as the cyber-attack took place in Bangladesh Bank. The fraudsters became successful in Bangladesh Bank heist as they had taken the advantage of consecutive holidays in Bangladesh (source bank nation), America (routing bank nation) and Philippines (destination bank nation). It is needed to understand that because of these consecutive holidays the reconciliation was delayed at Bangladesh bank and when the fraud was detected, they could not communicate with the routing bank in America on time. In our case we were lucky to get the chance of reconciliation on time and instantly communicated with the routing bank to block those 6 transactions. So the fraud was prevented by manual reconciliation and not by any cyber security system.

This is kind of threat is the emerging threat to our bank to keep our SWIFT terminals secured from any malware attack.

As per the branch manager of the ICICI bank the banking industry is constantly attacked by phishing campaigns, DDOS (Distributed Denial of Service), ransomware, malware etc. advanced
malware which is designed to target internal IT infrastructure of the bank is the emerging threat to the bank.

6. What kind of risk polices your bank has implemented to address the cyber security?

As per manager of Cosmos bank, they have collaborated with tech giant Infosys to beef up the IT infrastructure. Bank has also enhanced the security measure for the ATM switch server and SWIFT server. Training programs are being conducted to spread the awareness regarding cyber security among the employees. Strong spam filters are installed to prevent phishing and spam mails.

State bank of India has implemented Network Access Control (NAC) for the protection from cyber-attacks. NAC restricts the unauthorized access in the network by non-compliant devices. On the other hand ITSM (IT service management) has also been implemented to manage IT infrastructure BY SBI. All of the branches are subject to cyber security audit. State bank of India has also deployed ethical hackers who are continuously monitoring the IT infrastructure of the bank and giving suggestion for improving the same.

Yes bank has the Information security unit which is under Risk management unit to check the cyber-attacks. It has already collaborated with Fortytwo42 labs to enhance the cyber security. Yes bank also adopted PI-Control system to boost the cyber security system of the bank. It conducts security testing of IT infrastructure on regular basis. It also has Security operation center to monitor suspicious network traffic.

Union bank of India has created a dedicated team of IT professionals who are experts in cyber security matters. It has developed cyber security policy and information security policy. Union bank of India has already implemented next generation integrated operation centre for early detection of any kind of cyber threat. It follows the cyber threat hunting program which is engaged in analyzing various security systems and network logs to detect advanced threats for the internal IT structure.

ICICI Bank created a governance framework to secure the internal IT infrastructure which is a independent director led board committee. The bank has adopted ‘defence in depth’ strategy to boost the IT security, as per the bank official. The bank has created redundancy at various layers like- storage, server and network. There are IT command centres which follow the practice of 24*7 monitoring. These IT command centres are having state of the art tools. The bank is also having a cyber security policy which is approved by the board. They use to conduct the statutory audit of the IT system periodically to ensure that the things are functioning properly. The bank
official also informed that the bank is working on blockchain based system to handle the trade finance service.

7. How much your bank is spending on the research of cyber security?

None of the participants have answered this question as this information is confidential to the bank.

8. How would you frame the relationship between fraud, trust and the future of commercial banking?

As per the manager of Cosmos bank told that when Cosmos Bank had witnessed some amount of withdrawals as a result of panic among the customers. But as the money was credited in due course and certain steps were taken to enhance the cyber security, customers again started depositing money in our bank. Eventually as per the balance sheet the deposit base of our bank has increased by 3% in this financial year.

According to the chief manager of State bank of India, It is very important for the whole banking industry to make the customers confident that their money is safe with the banks. For the same the banks has to be take futuristic measures to counter the problem of cyber theft. Earlier in many cases we have witnessed withdrawal of money by customers who has experienced cyber theft. But this tendency is not seen today because of two reasons:

1. According to bank’s new policy, the money gets credited in the customer’s account within specific time period if bank is responsible for the cyber theft.

2. The technological innovations that State bank of India is constantly bringing to secure the hard earned money of the customers, has enhanced the trust.

Also SBI is continuously trying to make the customers more aware to avoid the cyber-attack while using internet and mobile banking.

Location head of Yes Bank had opined that the relationship between fraud and trust is completely inversely proportional. The more vulnerable any bank is regarding cyber threats, the less trustworthy that bank is. The relationship between the banker and customer is of trustee and beneficiary. At all cost the bank has to protect the money of the customers as that money is the demand liability to the bank. He also added that in future the banking industry will witness
increasing amount of online and mobile banking transactions. The habit of traditional branch banking is going to change forever. All the banks have to be futuristic to combat the threats towards online and mobile banking.

As per the senior manager of Union Bank of India, today the public sector banks are already low on their deposit base. Almost every year Indian government is funding the public sector banks with money. In such scenario, if the customers also panic because of the online fraud and start withdrawing money, then the public sector banks will be unable to carry out the banking business. That’s why the cyber threat is the most urgent issue that needs to be addressed by the public sector banks by enhancing cyber security at all verticals. As a result of security measures taken by Union bank of India, the deposit base has grown by 8% yoy.

The branch manager of Icici Bank opines that the future of banking is online banking and mobile banking which are most vulnerable to the cyber fraud. All the banks have to continuously enhance their security level to prevent the threat of fraud. In many cases confidential data of the customers use to get leaked from the third party agents which in turn helps the fraudsters to commit unauthorized transactions. So the third party agencies also have to constantly increase the level of security measures to tackle the cyber fraud issue. Banking is a service industry that runs on the trust of the customers. He also added that If at any point of time this trust evaporates, the whole banking system will collapse like house of cards along with the economy.
Chapter V

5. Discussion and Conclusion

In this section the researcher will try to analyze his research work to find answer to the research question. During the research the researcher has learnt a lot about the cyber frauds taking place in the banking industry.

At first researcher tried to understand the scale of cyber fraud in the Indian banking industry. It was found that the matter was so serious that the regulator of Indian banking system RBI had to intervene to solve this issue. There are plenty of reasons behind the intervention of RBI. The first and foremost was to enhance the trust among the customers on the banking system. If the customers lose their confidence on the bank then they will start withdrawing the money from the bank. The customers have plenty of options to park their fund like gold, equity, mutual fund (debt, equity and hybrid) etc. Now the main business of the bank is to collect fund from the customer in the way of current deposit and savings deposit at cheaper rate and then to lend that money to the industries, individuals at higher rate. The industry use to finance the working capital expenditure, project cost expenditure etc. from that money which in turn generates employment. The individual on the other side avails car loan, housing loan, personal loan etc. from the bank which generates demand for goods and services. If banks start losing their deposit base then their ability to lend money to the industry will fall proportionally which will hamper the growth of the industry as well as the growth of the economy.

Then the researcher studied the different ways to commit cyber fraud. Today hacking, phishing, pharming, vishing etc. techniques are used to commit online fraud. Newer techniques like debit card skimming, fake apps, sim swap have become more dangerous for the banks.

For the above stated reason the banks have come out with different technological solution to prevent this threat. Banks are adopting different technological advancement in the field of data mining, blockchain, artificial intelligence, machine learning etc. Today the whole SWIFT system
in the banks are being tried to get built on blockchain platform to avoid any kind of unauthorized transaction.

The researcher had conducted several interviews to complete the primary research of the dissertation. All the interviewees are professionals in the field of banking having more than 5 years of experience. A summary of answers given by the interviewees and what the researcher concluded from his research is discussed below.

1. **Has your bank been impacted by the cyber fraud?**

All of the participants had agreed that their banks are impacted by the cyber fraud. But the impact differs from bank to bank. Small commercial bank like Cosmos bank was a victim of cyber fraud worth Rs. 95 crore (12 million euros) which is a big amount for a bank which is having deposit base of only Rs. 15000 crore (1875 million euros).

After reading so much about the cyber fraud, the researcher also thinks that today all of the banks are adversely impacted by the cyber frauds. Some banks are directly losing money where as some banks detect the fraudulent activities at the early stage and are able to prevent it. Today many banks are outsourcing the services like ATM and POS. Customer data can get leaked by these third party agents also. The same thing happened with yes bank and even with India’s largest commercial bank State Bank of India.

2. **What are the primary sources/causes of cyber fraud?**

The interviewees gave different answers to this question. But most of them had agreed that the technological advancement is the main reason behind creation of advanced malwares which are difficult to detect. One of them pointed out the role of countries like North korea from where this kind of activities can take place easily. Eventually many of the cyber attacks have supposedly taken place from North Korea.

The researcher also thinks that the new technological innovations are the main reason behind this threat. The fraudsters need a safe haven to commit this kinds of frauds. Sanctioned countries like North korea is giving these fraudsters the much needed shelter. Another main source of this threat is the fake apps available at the google palystore. These apps looks exactly like the original one and use to lure people by giving some special offer on the installation. Once customer installs the fake app and start transacting from the same, all the confidential data like online banking password, ATM pin, CVV no. get compromised with the fraudsters. One more reason is the awareness among the customers. Today all of us irrespective of age, sex, educational background, location use the online banking and mobile banking because of which everyone does not follow the safeguards properly.
3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

While answering this question all the participants have given the same response. As all the banks are regulated by Reserve Bank of India, they follow the guidelines given by RBI. If the online fraud is reported within three working days to the bank, then the customer’s liability is zero and the money is credited within 10 days to the customer’s account by our bank. If the fraud is reported after 3 working days but within 7 working days, then the liability of the customer is Rs. 25000/- maximum depending on the type of the account. If the same is reported after 7 working days, then the liability of the customer is fixed by the internal policy of the bank.

Researcher also feels that it is the obligation for the banks to obey the guidelines given by the central bank regulator. If the particular guidelines is not followed then the customers have the option of lodging complaint against the respective bank at the ombudsmen section of the RBI. Earlier it was time taking, painful and uncertain process to recover the money by the customers from the bank which was stolen because of the cyber fraud where customers were not at fault. The customers also losing confidence about the safety of their assets because of this. That is why RBI had to come out with the guidelines in which it has defined the exact time by when the money will be credited to the customer’s account. This single move has boosted confidence among the customers to park their fund with bank.

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

Different banks have taken different policies in handling cyber fraud. Banks like State bank of India, Union bank of India have taken insurance policy to tackle the situation. Small private bank like Cosmos bank has made provision in their balance sheet against the cyber fraud. Whereas major private players like yes bank and Icici bank has neither taken any insurance policy nor they have provisioned any money for the cyber theft.

The researcher has also found that most of the banks today in India are taking insurance policies to minimize their losses. Demand for cyber insurance in India has already grew by 40% in 2018. The global cyber insurance market is expected to grow by $22.8 billion within 2024. Though the tendency of adopting cyber insurance policies is quiet low, but still about 350 cyber insurance policies was sold in 2018 where most of the buyers were banks. According to the “Allianz Risk Barometer 2019 study, businesses in India consider cyber fraud as the top risk. But it should also be noted that the insurance policies are not the alternative to the cyber security of any bank. If any entity approaches for the cyber security, then the insurer first evaluate the cyber security system of the bank. If the security system found to be strong then insurer provides better coverage for the entity. (DSCI Report, 2018)
5. What kinds of new/emerging cyber threats is your bank is experiencing?

The participants differ in answering this question also. Cosmos bank is encountering new kind of malware attack which attacks the ATM switch of the bank. State bank of India is facing a new type of attack called DDOS (Distributed Denial of Service) where the malicious traffic restricts the genuine traffic to go through to original application. Yes bank is facing the challenge of malware attacks which are specially designed to attack SWIFT terminals of the bank. Union bank of India is also facing a challenge to keep their SWIFT terminals secure from the malware attack. Whereas Icici bank is facing it challenging to keep their internal IT infrastructure of the bank from the malware attack.

According to the researcher more than 25% of all the malwares target banks more than any other industry. Trojan viruses are used for stealing information of the bank customers. Today more than 20 ATM malware families can be found around the globe. Ransomware is also a big headache for the banks today. Many of the banks were threatened by the ransomware attack of “wannacry” virus. Even the bank regulator RBI was so scared of this ransomware that it had instructed all the banks to update software systems at their ATMs with a security patch released by Microsoft Corp. as a precautionary measure in the wake of the ransomware attack triggered by the WannaCry virus.

6. What kind of risk polices your bank has implemented to address the cyber security?

Different banks have taken different steps to address this issue of cyber fraud. Like smaller player like Cosmos bank has collaborated with Infosys and bigger players like Yes bank has collaborated with Fortytwo42 labs to strengthen the cyber security measures. Cosmos Bank has also enhanced the security measures for their ATM switch server and SWIFT server. State Bank of India has taken measure to restricts the unauthorized access in the network by non-compliant devices via NAC (Network Access Control). They have also deployed ethical hackers. Union bank of India cyber threat hunting program.

As per the researcher, most of the banks have been able to protect their internal IT system from external malware/ransomware attack successfully as they have poured their significant resources towards this. But the problem lies where banks have to depend on third party agents. In India most of the ATMs and POS are operated by third party vendors like Hitachi payment services. The security system of these vendors are not strong as the security system of the banks. So the attackers has turned their focus towards these third party vendors. Another issue is the shared banking system. All of the banks use the shared banking system called “SWIFT” in which millions of dollar worth cross border transaction happens. The fraudsters has also targeted SWIFT, the example we can see in the Bangaladesh bank heist and the failed attempt to steal
money from Union bank of India. These are the areas where banks have to focus to reduce the risk of cyber attack.

7. **How much your bank is spending on the research of cyber security?**

None of the interviewees had answered this particular question as it is a confidential data of the bank.

As per the researcher, Indian banking system has spent more than $10 billion in 2018 which is almost 10% higher than the previous year. Banks are investing heavily on blockchain technology and artificial intelligence.

8. **How would you frame the relationship between fraud, trust and the future of commercial banking?**

As per the respondents, bank’s main objective should be to keep the money of the depositor safe with them. If the depositors find any difficulty in getting back their money, then they may turn their face from the bank to park their money.

As per the researcher, India is such a country where the savings propensity of the people is relatively higher than other developed countries. The household savings rate in India stood at 17.2% compared to USA at 7%, Canada at 1.69% and Eurozone at 5% (OECD Report. 2019). The simple reason behind this kind of behaviour is that Indian government does not provide any kind of “state pension” to the Indian citizens. So people use to save money for their post retirement age. That is why they become skeptical and lose the trust very fast on banks if they come to know about any cyber theft. Keeping all these things in mind the banks After all the whole banking industry runs on confidence and trust.

**Conclusion**

The main objective of the research is to find whether the technological innovation is enough to reduce fraud and increase trust in the Indian banking system. After reviewing some literatures and conducting some interviews the researcher comes to the conclusion that Yes the technological innovation is enough to reduce fraud and increase trust in the Indian banking system.
If trust would have evaporated from the banking system, then the banks would have seen the decline in deposit base. But we can see the bank’s deposit base has ultimately gone up instead of going down. Even the banks which were hit the most because of this cyber fraud has witnessed an uptick in their deposit base. In recent years all of the alternative routes where people can park their money like stocks, gold, mutual funds have given positive returns. But still people thinks that it is safer to park their fund in banks. On the other side banks are well aware about the sensitivity of the issue. That’s why they are putting maximum resources to secure their IT infrastructure from the cyber-attack. Some of the banks are hiring ethical hackers to cross check their security system. Many of the banks are collaborating with top most IT firms of the country to beef up the security system. In many cases the cyber-attacks were detected early and corrective actions were taken before losing any significant amount of money. The interference of Reserve bank of India also needs a mention as their guidelines to return the money of the cyber fraud victims within a stipulated time period, has played a key role to boost up the confidence level of the customers.

India is too big and the banks are aiming at providing the banking service to the every part of the nation. To facilitate this rapid expansion, banks need to outsource some of the services for which they deploy third party vendors to maintain ATMs and POS. These third party vendor are the “Achilles heel” of the Indian banking system. As the security system of the banks have become advanced and futuristic, the fraudsters now started attempting to attack the ATMs and POS maintained by the third party vendors. The security system in these third party vendors are not as advanced as the banks. In most of the cases the data breach happen from these ATMs and POS which are maintained by third party vendors.

**Recommendations**

As per the researcher, people of India is still having trust and confidence on the Indian banking system because of the new measures taken by the banks and RBI. The banks have stubborn IT security systems in place to counter the threat of cyber-attack. The only lacuna that persists in the system is the insufficient security measures taken by the third party vendors. There should be further research on this topic to find out clearer picture of the banking system.
Chapter VI

6. Personal Reflection

I researched and wrote my dissertation in 2019 along with the rest of the students of Masters of business administration at Dublin Business School. Initially it was very difficult for the researcher to choose the topic from the ocean of topics. It was only after the discussion with the supervisor, finally the researcher came with a unique topic which is actually a very important issue in respect to Indian banking system as well as Indian economy. The topic that was selected as followed:

"The potential of technological innovation to reduce fraud and increase trust in the Indian banking system"

After spending almost three months on the above mentioned topic, the researcher came to the conclusion that the technological innovation has indeed helped in reducing electronic banking frauds which has in turn increased the trust in Indian banking customers.

The researcher has learnt newer things happening around the world. Though the researcher was an ex banker by profession, but still he has a very limited idea about what kinds of frauds are taking place in the banking system and the banks are utilizing the might of technology to prevent them. While doing the secondary research the researcher had gone through many articles, websites, journals regarding this topic. Then only the researcher got some theoretical idea about the whole issue. Then he carefully selected the respondents for the interviews. The researcher tried to take the view from the officials from the different kinds of banks like- small scheduled bank, large and medium public sector bank, large and medium private sector bank to get the sense of the things happening practically in the banking industry. To get the interviews of the bank officials were not easy as all of the respondents are either manager or above manager levels in their banks. The time management skill of the researcher has got enhanced while fixing the time with these officials and taking interviews.
Reflection on learning background

Experiential learning is a powerful approach to address an individual's overall development, though the learning depends on the inclination, style, qualities of the individual.

The experiential learning works on two stages: a four stage learning cycle and four separate learning style. The very first step of the experiential learning cycle is the concrete experience. In this step a new experience/ situation is encountered. The next stage is reflective observation of the new experience where reflective skills to these new experiences can be viewed from a variety of perspectives. The very next strategy is abstract conceptualization where integrative ideas and concepts can be created from their observations. The last stage is called active experimentation where new concepts can be used in practical scenario.
Development of learning and performance

The learning and performance process started from one year back when he arrived in Dublin to pursue MBA finance. The first challenge for the researcher was to adopt the new culture and weather of Ireland. The second challenge was the food as it was totally different from the researcher’s native country India. Though the researcher has a good experience in finance field but the style of education in Ireland is bit different in Ireland. The education system is more application based whereas in India it is more theoretical based. But with the support of the teachers, the researcher adopted the newer things quietly.

Being an ex banker the banker had an idea about the threat of cyber fraud in Indian banking system. After choosing this topic the researcher started reading different journals, websites to have a better idea regarding the topic. Then to get a practical sense of this issue, the researcher conducted five interviews of different bank officials.

With the help of the analytical skill along with his study regarding the topic and interviews, the researcher completed the research.
Bibliography


10. Charan Singh, Frauds in the India banking industry; 2016


15. Dr Madan lal Bhasin (2016) : The Fight Against Bank Frauds: Current Scenario and Future Challenges: Ciencia e Tecnica Vitivinlcola, ISSN: 0254-0223

16. Dr. Sukhamaya Swain, Dr. Lalata K Pani (2016); Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures


30. S.N. John, C. Anele, O. Okokpuje Kennedy et al (2016), Real time fraud detection in the banking sector using data mining techniques/algorithim, International Conference on Computational Science and Computational Intelligence, doi: 10.1109/CSCI.2016.0224

31. Reserve Bank of India, Master circular dated 03 july, 2017, Classification and Reporting by commercial banks and select FIs


34. Shailak Jani (2018), An Overview of Ripple Technology & its Comparison with Bitcoin Technology


39. Wei Wei· Jinjiu Li· Longbing Cao, (2012), Effective detection of sophisticated online banking fraud on extremely imbalanced data, ISSN: 1386-145X

Appendix

Appendix A:

Question:

1. Has your bank been impacted by the cyber fraud?

2. What are the primary sources/causes of cyber fraud?

3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

5. What kinds of new/emerging cyber threats is your bank is experiencing?

6. What kind of risk polices your bank has implemented to address the cyber security?

7. How much your bank is spending on the research of cyber security?

8. How would you frame the relationship between fraud, trust and the future of commercial banking?
Appendix B: Interviews

Participant position: Manager (IT)
Work experience in banking industry: 6 years.
Name of the Bank: Cosmos Bank
Country: India

1. Has your bank been impacted by the cyber fraud?

Yes we are heavily impacted by cybercrime. In the fiscal year 2018 we had faced an incidence of cyber fraud in which Rs. 95 crores was theft from our bank. It was a very big hit as we are a very small bank with deposit base of only Rs. 15000 crores. Apart from this incidence customers have reported almost 100 online fraud cases of which most of the transactions were below Rs. 1 Lakh.

2. What are the primary sources/causes of cyber fraud?

Technological advancement. Also I would like to say that may be countries like North Korea is becoming the main source from where these online frauds are getting organized. The major cyber attack of 94 crore that we had faced, was originated in North Korea. The culprits behind the Bangladesh cyber fraud also organized their crime from the same country.

3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

We follow the Reserve bank of India guidelines which says that if the complaint is filed within three days then the bank will credit the customer’s account within 10 working days from the date of notification by the customer.

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

Yes. As per the reported balance sheet, our bank has provisioned Rs. 18 crore for cyber fraud.

5. What kinds of new/emerging cyber threats is your bank is experiencing?
In the fiscal year 2018 we had faced a fraud of Rs. 95 crores which was done via malware attack on our main server. The attackers entered into the network by sending spear phishing mail. Once malware was inserted into the system, it sets up ATM/POS proxy switch which was in parallel with bank’s own central switch. The connection between the core banking system and bank’s central switch was then redirected because of which the required messages to authorize debit card withdrawals never got forwarded to the core banking system. So the card number, pin etc. could not have been checked by the core banking system. On the other hand fraudulent messages were sent from the malicious switch to authorize fraudulent transaction. Many of the ATM cards were cloned and money was withdrawn in various ATMs in different countries. This type of attack in which a proxy switch was generated by inserting a malware, was new to us.

6. **What kind of risk polices your bank has implemented to address the cyber security?**

Our bank has collaborated with Infosys to beef up the IT infrastructure. Bank has also enhanced the security measure for the ATM switch server and SWIFT server. Training programs are being conducted to spread the awareness regarding cyber security among the employees. Strong spam filters are installed to prevent phishing and spam mails.

7. **How much your bank is spending on the research of cyber security?**

This information is confidential.

8. **How would you frame the relationship between fraud, trust and the future of commercial banking?**

Initially when the cyber attack had happened our bank had witnessed some amount of withdrawals as a result of panic among the customers. But as the money was credited in due course and certain steps were taken to enhance the cyber security, customers again started depositing money in our bank. Eventually as per the balance sheet the deposit base of our bank has increased by 3% in this financial year.
1. **Has your bank been impacted by the cyber fraud?**

   Yes, our bank was impacted by cyber frauds in the past. In 2016 our bank had encountered a massive cyber-attack in which malware induced security breach for which information about almost 0.6 million debit cards was leaked. Immediate action was taken by blocking the debit cards and re-issuing them. Also our bank is facing issues with card cloning, card skimming etc. We have controlled the menace of phishing mail which was a big headache for us.

2. **What are the primary sources/causes of cyber fraud?**

   One of the primary sources of the cyber fraud is “Google play” app where fake banking apps are present in numbers. Once customers install the fake app in their mobile, all the personal data of the customer gets compromised with the fraudster. Actually it is very difficult to identify these fake apps as they are very close copy of the original one. Sometimes they mimic the exact graphic design of the original app. Another reason is the awareness among the customers. They sometimes do not take the proper measures to keep the personal data confidential and the same gets compromised with the fraudsters.

3. **What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?**

   Being a part of the banking system, we follow the guidelines given by Reserve Bank of India. If the incidence of online fraud has taken place due to negligence of the bank and the same is reported within 3 days then, within 10 days the money will be credited to the customer’s account. If a “third party” breach happens then also bank is liable to pay if the fraudulent transaction is reported within 3 days.

4. **Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?**

   Yes. Our bank has taken an insurance policy worth $100 million to cover cyber risk.
5. What kinds of new/emerging cyber threats is your bank experiencing?

We are experiencing a new type of attack called DDOS (Distributed Denial of Service) where the malicious traffic restricts the genuine traffic to go through to original application. Once this attack becomes successful in penetrating the firewall, it infects the core banking system.

6. What kind of risk polices your bank has implemented to address the cyber security?

Our bank has implemented Network Access Control (NAC) for the protection from cyber-attacks. NAC restricts the unauthorized access in the network by non-compliant devices. On the other hand ITSM (IT service management) has also been implemented to manage IT infrastructure. All of our branches are subject to cyber security audit. Also our bank has deployed ethical hackers who are continuously monitoring our IT infrastructure and giving suggestion for improving the same.

7. How much your bank is spending on the research of cyber security?

I cannot tell the amount but can say that our bank is investing heavily on cyber security by hiring security experts in big number. Also we have partnered with Oracle for the cyber security matter.

8. How would you frame the relationship between fraud, trust and the future of commercial banking?

It is very important for the whole banking industry to make the customers confident that their money is safe with the banks. For the same the banks has to be take futuristic measures to counter the problem of cyber theft. Earlier in many cases we have witnessed withdrawal of money by customers who has experienced cyber theft. But this tendency is not seen today as according to our new policy, the money gets credited in the customer’s account within specific time period if bank is responsible for the cyber theft. Also we are trying to make our customers more aware to avoid the cyber attack while using internet and mobile banking.
Has your bank been impacted by the cyber fraud?

Yes we are impacted by cybercrime. In the fiscal year 2016 we had faced a major data breach of 3.2 million ATM card holders from POS (point of sale) terminals and ATMs which were managed by Hitachi payment services limited. The financial loss was restricted by blocking those infected cards and reissuing them. Apart from that incident, we are facing attacks like card skimming, card cloning etc. in our ATM network. In the last financial year, we had received almost 800 cases regarding fraudulent transactions by ATM cards.

What are the primary sources/causes of cyber fraud?

Our ATMs and points of sales are managed by third party agencies (like Hitachi payment services). There are always chances of data breach from their end as it happened in 2016. Another main source is the fake apps of Yes bank available in “Google play store”. Customer installs the fake apps and falls prey to the fraudsters. Also the rapid advancement of technology is responsible for the same.

What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

We are following the guidelines given by Reserve bank of India. If the online fraud is reported within three working days to the bank, then the customer’s liability is zero and the money is credited within 10 days to the customer’s account by our bank. If the fraud is reported after 3 working days but within 7 working days, then the liability of the customer is Rs. 25000/- maximum depending on the type of the account. If the same is reported after 7 working days, then the liability of the customer is fixed by the internal policy of the bank.

Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

Currently our bank has done no provisioning for the cyber frauds.

What kinds of new/emerging cyber threats is your bank is experiencing?
Recently we have encountered with a new kind of malware specially designed to attack our “SWIFT” terminals which was sent by a malicious mail. It is because of our advanced security measures, the attack was failed. After the Bangladesh bank heist, the attackers have turned their focus on “SWIFT” terminals as high value cross border transactions take place via “SWIFT”.
We are also experiencing new types of malwares which target the components of the internal IT infrastructure of the bank like operating system, databases, files, firewalls etc. These malwares are getting technologically advanced day by day.

6. **What kind of risk polices your bank has implemented to address the cyber security?**

Our bank has Information security unit which is under Risk management unit to check the cyber-attacks. Our bank has already collaborated with Fortytwo42 labs to enhance the cyber security. We have adopted PI-Control system to boost the cyber security system of the bank. Our bank conducts security testing of IT infrastructure on regular basis. Our bank has Security operation center to monitor suspicious network traffic.

7. **How much your bank is spending on the research of cyber security?**

This information is confidential.

8. **How would you frame the relationship between fraud, trust and the future of commercial banking?**

The relationship between fraud and trust is inversely proportional. The more vulnerable your bank is regarding cyber threats, the less trustworthy your bank is. The relationship between the banker and customer is of trustee and beneficiary. At all cost the bank has to protect the money of the customers as that money is the demand liability to the bank. In future we will see an increasing amount of online and mobile banking transactions. The habit of traditional branch banking is going to change. All the banks have to be futuristic to combat the threats towards online and mobile banking.
Participant Position: Senior Manager
Work experience in banking industry: 10 years
Name of the bank: Union Bank
Country: India

1. Has your bank been impacted by the cyber fraud?

Our bank is impacted by the cyber fraud. In 2016 we had encountered a major cyber-attack which was intended to steal $171 million by the hackers. It was the biggest online fraud our bank had ever faced. Our bank had reported almost 50 cases of ATM frauds in the last financial year. In most of the cases card skimmers were used to do the fraudulent transactions.

2. What are the primary sources/causes of cyber fraud?

The main cause of the cyber fraud is the changing habit of the customers to bank. Today customers like online and mobile banking instead of going to branches physically. This transformation has taken place without proper knowledge of taking precautions. The fraudsters exploit this loophole and become successful in their intension of stealing money. One more reason is the advancement of technology. Because of newer types of malwares, it has become very difficult for any bank to detect and prevent them from infecting the system.

3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

We are following the guidelines given by Reserve bank of India. If the online fraud is reported within three working days to the bank, then the customer’s liability is zero and the money is credited within 10 days to the customer’s account by our bank.

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?

Our bank has taken cyber liability insurance of Rs. 325 Crore.

5. What kinds of new/emerging cyber threats your bank is experiencing?
As discussed earlier our bank had experienced a cyber attack which was attempted to steal $171 million in 2016. At first a malicious email containing the malware as attachment, was sent from an authentic source – RBI (Reserve bank of India) to many of the employees. The attachment was in a zip file which was dot (xer) file instead of dot (pdf) file. As soon as one of the employees opened up the email, the malware got released in the system and the fraudsters got access of credentials of the SWIFT. By login into SWIFT account the hackers had been able to send $171 million to the banks in Cambodia, Thailand and Australia which was routed through Citibank New York and JP Morgan Chase New York. They had also tampered with SWIFT’s prt file where they had deleted those 6 entries of the fraudulent transactions. When the very next day the SWIFT transaction report came and reconciled, it was found that $171 million was stolen from the dollar nostro account. Immediately the money trail was traced and the transaction was blocked. Thus our bank did not incur any lose because of this attack. The modus operandi of the attack was same as the cyber-attack took place in Bangladesh Bank. The fraudsters became successful in Bangladesh Bank heist as they had taken the advantage of consecutive holidays in Bangladesh (source bank nation), America (routing bank nation) and Philippines (destination bank nation). It is needed to understand that because of these consecutive holidays the reconciliation was delayed at Bangladesh bank and when the fraud was detected, they could not communicate with the routing bank in America on time. In our case we were lucky to get the chance of reconciliation on time and instantly communicated with the routing bank to block those 6 transactions. So the fraud was prevented by manual reconciliation and not by any cyber security system. This is our new threat to keep our SWIFT terminals secured from any malware attack.

6. What kind of risk polices your bank has implemented to address the cyber security?

As told earlier that our bank has already taken an insurance policy to mitigate the risk of cyber attack. Our bank has created a dedicated team of IT professionals who are experts in cyber security matters. We have developed cyber security policy and information security policy. Our bank has already implemented next generation integrated operation centre for early detection of any kind of cyber threat. Our bank also follows the cyber threat hunting program which is engaged in analyzing various security systems and network logs to detect advanced threats for the internal IT structure.

7. How much your bank is spending on the research of cyber security?

This information is confidential.

8. How would you frame the relationship between fraud, trust and the future of commercial banking?
Today the public sector banks are already low on their public deposit base. Almost every year Indian government is funding the public sector banks with money. In such scenario, if the customers also panic because of the online fraud and start withdrawing money, then the public sector banks will be unable to carry out the banking business. That’s why the cyber threat is the most urgent issue that needs to be addressed by the public sector banks by enhancing cyber security at all verticals.
1. Has your bank been impacted by the cyber fraud?

Yes, our bank is also impacted by the cyber fraud. We are most affected by the application of skimmers in the ATM machines. In the last year almost 120 cases of were reported where money was stolen from ATM as the ATM skimmer was attached to the ATM machine. Also phishing mail is a big issue for our bank.

2. What are the primary sources/causes of cyber fraud?

One of the main sources of cyber fraud is the fake apps available at google play store. They use to appear same as the original bank app. Customers erroneously downloads the fake app and start transacting with the same. Thus the confidential banking data gets compromised with the fraudsters. Customer awareness is also a reason why people lose money because of the cyber frauds. Today people of all age group and gender use the alternative channels like ATM, online banking. But many of them still not follow the safeguards which give the fraudsters the chance to steal money fraudulently.

Another reason is the advancement in the technology. Because of the advancement, newer malwares, techniques are getting developed to commit the fraud.

3. What is the policy of your bank when an individual files a complaint regarding monetary loss resulting from online fraud?

We are following the guidelines given by Reserve bank of India. If the online fraud is reported within three working days to the bank, then the customer’s liability is zero and the money is credited within 10 days to the customer’s account by our bank. If the fraud is reported after 3 working days but within 7 working days, then the liability of the customer is Rs. 25000/- maximum depending on the type of the account. If the same is reported after 7 working days, then the liability of the customer is fixed by the internal policy of the bank.

4. Does your bank make, or plan to make, any provisions for the monetary losses due to online frauds?
No, our bank has not done any provisioning for the monetary losses occurred due to online fraud.

5. **What kinds of new/emerging cyber threats is your bank is experiencing?**

Advanced malware which is designed to target internal IT infrastructure of the bank. These malwares get inserted into the system getting unnoticed by the security system in place. After it penetrates into the internal system the confidential data gets compromised with the fraudsters. The security measures taken by the bank has to be futuristic to counter this threat.

6. **What kind of risk polices your bank has implemented to address the cyber security?**

ICICI Bank created a governance framework to secure the internal IT infrastructure which is a independent director led board committee. The bank has adopted ‘defence in depth’ strategy to boost the IT security, as per the bank official. The bank has created redundancy at various layers like- storage, server and network. There are IT command centres which follow the practice of 24*7 monitoring. These IT command centres are having state of the art tools. The bank is also having a cyber security policy which is approved by the board. They use to conduct the statutory audit of the IT system periodically to ensure that the things are functioning properly. The bank official also informed that the bank is working on blockchain based system to handle the trade finance service.

7. **How much your bank is spending on the research of cyber security?**

I cannot disclose the figure.

8. **How would you frame the relationship between fraud, trust and the future of commercial banking?**

Future of banking is online banking and mobile banking which are most vulnerable to the cyber fraud. All the banks have to continuously enhance their security level to prevent the menace of fraud. In many cases confidential data of the customers use to get leaked from the third party agents which in turn helps the fraudsters to commit unauthorized transactions. So the third party agencies also have to constantly increase the level of security measures to tackle the cyber fraud issue. Banking is a service industry that runs
on the trust of the customers. He also added that if at any point of time this trust evaporates, the whole banking system will collapse like a house of cards along with the economy.

Appendix 2:

**Ethics Information – Business Postgraduate Studies**

<table>
<thead>
<tr>
<th>Student Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Identifier:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Submission Date:</td>
</tr>
<tr>
<td>Proposal Research Title:</td>
</tr>
<tr>
<td>Brief Description of the research:</td>
</tr>
</tbody>
</table>

**Sampling**

<p>| Population of interest: | Bank officials. |</p>
<table>
<thead>
<tr>
<th>(brief description)</th>
<th>Being an Ex bank manager it is possible for me to collect the responses from senior bank officials.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample of interest:</td>
<td>Sample size – 5</td>
</tr>
<tr>
<td>(brief description of size and how it is chosen)</td>
<td></td>
</tr>
</tbody>
</table>

### Primary Research - Data Management

<table>
<thead>
<tr>
<th>Is the data anonymised – how is this done?</th>
<th>Yes. Data is anonymised by keeping the details of the responder confidential.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How is data confidentiality maintained:</td>
<td>By keeping the details of the responder confidential.</td>
</tr>
<tr>
<td>Where will the data be stored:</td>
<td>Data will be stored in my personal laptop and in college server.</td>
</tr>
<tr>
<td>When will the data be destroyed:</td>
<td>The day after the time period for appeal-of-grade period has expired.</td>
</tr>
</tbody>
</table>

### Specific Ethical Considerations

<table>
<thead>
<tr>
<th>Detail any aspects specific to your proposal that will require further ethical approval e.g. interaction with under-18 year-olds,</th>
<th>NA</th>
</tr>
</thead>
</table>
experiments requiring deception, anything that might cause respondents any distress, etc.

Student Signature: Subhajit Routh
Date: 26.08.2019
Signed: Subhajit Routh