

Analysis of financial frauds in electronic payment systems in India and China

Arnab Chatterjee ^a

^a Symbiosis Institute of Management Studies, Symbiosis International (Deemed University), Range Hills Road, Khadki, Pune, 411020, Maharashtra, India

Abstract

This paper aims to study various fraud occurrences in India and China and their outcomes on the general public. Financial transactions have become easy since the invention of internet, but some miscreants called fraudsters are using it for unlawful activities which causes huge financial losses worldwide every year. The results of this research can be used by financial organizations around the world for customer's awareness and education and also in making better policies for protecting the citizens and bank from financial frauds in respect of financial activities, geographical location and its usage. In both the countries used to conduct research the quotative data is being used to test the fraud occurrence model. The results from this research helps us in understanding different behaviors of customers regarding online transactions and frauds associated with them. It was noted that in China, the satisfaction level of customers was relatively less and service quality was not up to the expected mark in the majority of situations. After conducting this research, the study suggests that a number of areas for improvement in the near future, especially related to fraud detection. If we can research the problems from the financial institution side rather than the consumer's side we can come up with better solutions to frauds as these institutions deal with fraud on a regular basis. The aim of the paper is to create a precise and statistical occurring globally and understanding of various frauds by using three approaches (geographical factors, IT usage and financial activities).

Keywords : Banking system, electronic commerce, Consumer behavior, Information security, Cyber fraud

INTRODUCTION

Banks have been helping human society for further progresses during last many centuries especially in the western world. Financial services that are provided to customers which are extremely small scale in nature like the cheque, credit cards etc, are called as personal or retail banking (Casu et al., 2006). In recent times due to advancement in technology the banks have been able to cater various needs of customers in different areas. The current advancement in technology has helped the customers by providing the latest solutions which cater to their various banking needs globally (Hanafizadeh et al., 2014); (Nguyen et al., 2012a). In the Asian community China banks have had a very short presence, so the products offered by banks are extremely new to the people of mainland China. However, in recent years, the Chinese people and the government has been trying to catch up to the banking standards of the western world. There was a famous article in the Indian express, at least one in every 10 million people in India has either lost money in a fraudulent scheme or know somebody who has fallen prey to such activities. When we compare China's banking system to the rest of the world it seems to be still in its nascent stages. Since the Chinese economy is just beginning to boom it is interesting to see whether they are also facing the same problems that well-established banks in the western worlds faced decades ago.

Literature Review

As per Chinese central bank records (PBC, 2010), Chinese people were able to use the first bank card in the year 1979 and this project was carried out in only a select few societies. This project was carried out in secret with the majority of the Chinese population being completely unaware of the project carried out by their government. In the last few decades there has been a complete overhaul in the banking system of China and by the year 2009, the Chinese people had 1,180 million cards in circulation in the whole country. The total number of credit cards used by the people were 18.7 crores. (Qi et al., 2016) found that, the people who choose to use these cards were fairly a young group and they were very different from their parents. The early adopters of these cards liked to travel abroad and they did not like the idea of using cash at every possible place since it was quite bothersome. These young people preferred the convenience of carrying cards and the benefits it offered. Since the invent of the internet, the banking payment system has become even faster compared to the pre internet period. (McKenna & Green, 2002) suggested that there are 4 factors that helps anybody differentiate between an internet interaction and physical contact: (1) higher confidentiality; (2) the decrease in importance of physical appearance; (3) higher flexibility with respect to time and extent of interaction; and (4) the extended abilities of social media. In short, the people who are using the internet for their everyday transactions are using it for the hassle-free environment and the fast pace options. The important thing to note here is that the greater concealment provided by the internet misleads some people to believe they are immune to any type of frauds since the internet will be protecting them. However, reality is far from this belief. (Joinson, 2001) suggested that communications in which computers are involved and the general behavior associated with the internet requires a high level of disclosures of personal information. (Nguyen et al., 2012b) had compared the interactions associated with online mode vs offline mode disclosures that a user has to make by investigating many factors which included communication methods, reason for interaction and relationships between communicators. (Grazioli, 2004) had explained that, people in general have a tendency to compare the new information with the information they already possess. It is quite unfortunate that we make this comparison to the people living on earth for many centuries, the internet in this comparison is extremely new and has many uncertainties associated with it. (Logsdon & Patterson, 2009) had discovered that there is highly unethical contacts and behavior established on the internet. RBI had released statistics in 2018 which showed that, loss due to fraud in INDIA had reached Rs.70000 crores in the year ranging from 2014-2018. As mentioned in one of the current studies organized by NSSO in 2017, the INDIA Payment Association, fraud losses from 2012 have been increasing for the Internet and bank cards. Figure 1 represents the losses in INDIA which had reached Rs. 3 crore 88 lakhs in 2012. A recent by RBI had said that as of in the first 4 months 2021 there was a total of 7400 fraud cases registered. There are about 5 crore 80 lakhs credit card users as of August 2020 and it is increasing at a regular pace every year. It is a matter of great concern for the authorities that as the number of credit card users increase the financial literacy of the consumers regarding these products is not increasing the same rate and these types of consumers usually face fraudster attacks in the future. There are various categories of fraud and there are ups and downs in each category as the technology to combat those frauds evolve over time. In 2012, the frauds which caused most losses to the Indian public were Card-not-Present. INDIA is a major country which advocates the use of Chip and PIN globally. If we exclude the cases against fraud, financial organizations benefit greatly as there is liability shift. If there was a payment done which was found to be fraudulent the liability of the frauds fall on the shoulder of the acquirer and the merchant is then held liable by the acquirer, given that the merchant is not chip and PIN-enabled. Since payment systems had started the Chip and pin is recognized as the biggest evolution since decimalization 35 years from 1997-2003 in the Indian subcontinent. China even today still uses bank cards that have been equipped with a six-digit pin and magnetic strip. Any online transaction in China in POS terminals, the cards issued by the banks needs to be used and then a correct PIN number needs to be entered to complete the payment transaction. The majority of the financial organizations in China have realized the benefit from these new Chip and PIN system, and are actively working towards its installation and replacement Since China has a huge population complete replacement of the existing cards is going to be a time and resource consuming process. Indian citizens while using online methods for payment submit credit/debit card details, like card number, card owners name, date of expiry, postal address, issue number/security code, etc., on the websites of online merchants. Indian customers have the flexibility to make an online purchase without having to use online financial services. Chinese online shopping on the other hand is very different and complicated because right from the beginning of any transaction online banking is

involved. Online users experience an increased level of security. Different financial organizations in China offer different solutions for online shopping security solutions:

- OTP generator/digital certificate: People using Mobile banking are being proposed to use OTP and biometric information to make the transactions secure (Tsai et al., 2012).
- Instant alert service which was started in 2006 by the China Construction Bank, which is one of the biggest four government operated Chinese banks, partnered with Chinese state-owned company China mobile to work on the instant messaging service.
- Virtual keyboard: customers can get extra protection from different viruses and trojans by using virtual keyboard, as these tend to record different numbers and characters which are being typed through a computer keyboard.

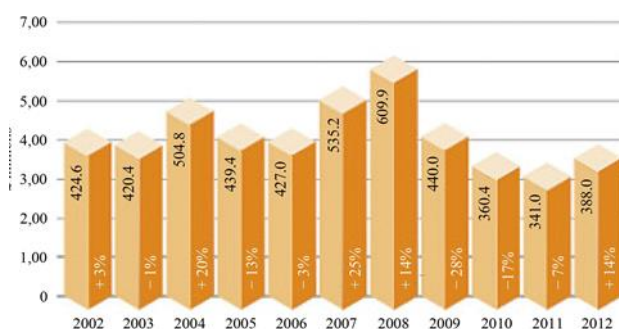


Figure 1. Debit/credit card losses in INDIA-issued cards 2002-2012

Conceptual background

For decades, people have been trying to investigate the theories that have been applied for innovation adoption. The most accepted technology acceptance model is (TAM;(Davis1989, n.d.) and innovation diffusion theory (IDT; (E. M. Rogers et al., 2019). The principal approach to study various methods of technology adoption and innovation was provided by TAM and IDT. It is interesting to see that as the time passes on technology have become customer-orientated and people-centered. It is extremely important to shift our attentiveness from system analysis to users one selves. There are a few variables based on TAM and IDT, used for testing purposes like the relative ease of use, customers perception on technology. The survey was carried out in both countries through the help of google forms and then the data was analyzed both qualitatively and quantitatively. Geographical factors were analyzed to understand the dawdling of promotion of technology in the Indian subcontinent. NSSO had studied the geographic characteristics which included age, income, education level and financial products ownership. People who fall into bracket of 35-54 years of age who have a higher chance of accepting internet banking services. Comparing this situation to India it was found that the credit card use in China, was mainly targeted towards individuals who were in the less than 26 years old and these people loved to take risks and see innovative financial solutions. This study showed that people who are using cards in China are relatively young when compared to the rest of the Asian counties and like the hassle-free environment provided by these cards. They were mainly attracted by the fact that the risk and hassle in carrying cash could be overcome significantly. The other studies conducted were mainly to find out the perspectives of the non-users of technology and their reasons for doing so. (Black et al., n.d.)in his research found that perceived risk was an important factor for individuals to use banking technology services while choosing services from different banks.(Mäenpää et al., 2008) and (Agarwal et al., 2009) suggested what subsequent research should be on regrading adoption of financial services and how it should go beyond our traditional approach. Although probable danger and issues related to security have been raised in previous studies (Rotchanakitumnuai & Speece, 2003),(Martins et al., 2014) believe that a true picture of the individuals suffering from individual fraud has yet not come into light and more study needs to be done regarding these. The interesting thing to observe is that it is quite obvious about the research gaps and what influential factors lead to financial frauds and their larger impact on society. When research was conducted into other internet frauds and the financial transaction involved in it was noted that a new field of study has evolved, which

includes data security, internet protocols, constructions. (Tzeng et al., 2005). New models are being continuously developed for providing greater security to consumers and rescues financial frauds. (Lin & Hsu, 2011) (Vincent et al., 2010). This research phase is being principally led by computer science individuals, but this study also helps us in understanding the IT usage of various people. The characteristics of internet and data transmissions has helped us in this study. This study contains IT usage of bank customers, particularly during online transactions which possesses potential threats to bank customers and also the banks themselves. The 3 approaches were combined for this study to understand the statics of occurrence of online fraud. Figure 2 represents the conceptual framework

Research hypothesis

Three approaches are introduced in this section which are centered on the conceptual model which was instigated in the earlier segment, demographical factors (Quazi & Talukder, 2011), economic activities (Nasri & Charfeddine, 2012) and IT usage (Buzetto-Hollywood, 2014), has been used to find out about fraud occurrences during transactions in the online mode. Variables and Research hypotheses are progressed in Section 4.1- 4.4.

4.1 Demographical factors

The data from demographics were greatly used in the 1980s in retail sectors (D. Rogers, 1986). Data obtained from demographics have been used to formulate marketing strategies for various subgroups of the population (Pol, 1986). During recent years, (Powers & Sterling, 2008) recommended that data which are obtained from demographics and which are relevant can be used to form strategies according to various customer segments. Therefore, the hypotheses associated to demographical elements are prepared as follows:

- H1. The occurrence of internet frauds is associated with different age groups.
- H2. The frauds which occur on the internet is associated with gender difference.
- H3. The frauds which occur on the internet is associated with difference in education levels.

4.2 Economic activities

A prototype was built by (Mckechnie, 1992) which helped in creating an interaction model to understand end-user behaviors when buying online and the long-term relationship of buyer-seller. So, the hypothesis which involves financial activities are as follows:

- H4. The frauds which occur on the internet is associated with bank card usage.
- H5. The frauds which occur on the internet is associated with usage of banking channels.
- H6. The frauds which occur on the internet is associated with the accounting management.
- H7. The frauds which occur on the internet is associated with customer satisfaction.

4.3 IT usage

Various activities are carried out in the internet with the invent and development of network technology. On a daily basis individual have been using the platforms for sharing data and also its transmission. Gralla (2006) studied various kinds of attacks that are possible on the internet like phishing attack browser weakness etc. The following hypotheses demonstrates a few popular activities associated with the individual's IT usage:

- H8. The frauds which occur on the internet is associated with the difference in the IT skills of individuals.
- H9. The frauds which occur on the internet is associated with IT usage frequency.
- H10. The frauds which occur on the internet is associated with online activity

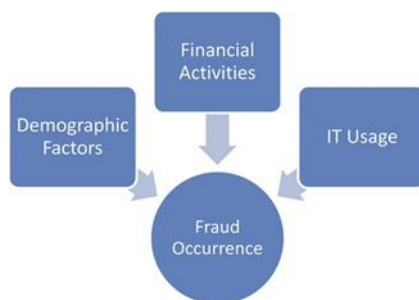


Figure 2. The conceptual framework

Research methods

5.1 Estimation development

(Hoehle et al., 2012), suggested researchers to use survey questionnaires to understand the customer's satisfaction of any service. A majority of quantification and variables are created based on earlier research but with a current touch. The questionnaire was divided into 4 parts which included private information of customers, IT usage, information on fraud cases (optional). The 4th section was exclusively designed for customers who had experienced related fraud and was thus left optional. A pre-survey was conducted on a sample size population of about 250 people in the Sothern part of India. In total 76 responses were received and then the responses were evaluated in understanding any difficulties or any vagueness in the questions designed for them. After this experiment a few changes were made as per responses from our test group.

5.2 Data collection

After the successful completion of initial research, the main questionnaire assessment was executed in the south Indian region in the form of google form survey. 1200 copies of survey were sent to various groups and residential areas for a period of 6 weeks. 272 valid responses and 13 uncompleted responses was received in the upcoming 6 weeks. SPSS was used for the interpretation of data and after all the responses were scrutinized manually. Due to ethical reasons, there was no follow up with the respondents once the responses were received. The survey was economized to safeguard the private data of the interviewee. There was a different method of data collection used in China due to confidentiality laws imposed by the government. The method to collect data was very different in both Countries. A local bank which wished to remain anonymous was approached for helping us with the collection of data. The banks database was used to contact to residents who were having or have used debit/credit card in the past. The survey was sent to 500 people as per bank's database and 189 people choose to reply back. However only 143 responses got completely filled, hence providing us a feedback value of 28.4 percent.

Data Analysis

Data analysis contains two sections. Geographic data for both the countries were compared first and then model building was completed using statistical tests which were relevant.

5.3.1 Geographic data of respondent from INDIA and China.

Based on Demographical data 4 variables were selected to represent both the countries: age, gender, education qualification and academic attainment (IT/finance related). The number of complete responses in Indian consumers is 272 and from the Chinese consumers is 143. The overview of 2 data sets is shown in table 1. To describe the age distribution in both countries 7 ranks were introduced. It was observed that in India, the data was collected for all the seven ranges but in the case of China it was different as data was mainly collected from four out of seven ranks. When professional in the industry were interviewed, we came to know that in Chinese bank services promotion are discouraged for the age group of people less than 20 years old and people who are above 60.

Table 1. Demographical data of respondents in India and China

<i>Variables</i>	<i>INDIA</i>		<i>China</i>	
	<i>Count</i>	<i>(%)</i>	<i>Count</i>	<i>(%)</i>
<i>Age (years)</i>				
< 20	2	0.7	0	0
21-30	22	8.1	74	52.1
31-40	32	11.8	54	37.3
41-50	57	21.0	10	7.0
51-60	48	17.7	5	3.5
61-70	50	18.5	0	0
> 71	61	22.1	0	0
Total	272	100	143	100
<i>Gender</i>				
Male	144	52.8	74	52.1
Female	128	47.2	69	47.9
Total	272	100	143	100
<i>Qualification</i>				
No formal qualification	21	7.7	4	2.8
GCSE/0 level	46	17.0	3	2.1
A level	25	9.2	12	8.5
BSc/BA	111	41.0	93	64.8
Further qualification	58	21.4	29	20.4
Not known	11	3.7	2	1.4
Total	272	100	143	100
<i>IT/Finance-related</i>				
Neither of them	223	82.3	57	39.4
IT-related	18	6.6	9	6.3
Finance-related	24	8.5	61	43.0
Both of them	7	2.6	16	11.3
Total	272	100	143	100
Incidents of actual financial fraud	58	21.4	7	4.9
Total	272		143	

When both the data sets for the variable gender was compared no significant difference was observed. When the qualification variable was compared in both data sets it was observed that majority of the respondents has graduate level qualification. It was observed that, academic level of participants (IT/finance related) conveyed some dissimilarity as follows: 82.4 per cent answerers in the INDIA have an academic experience which was not in relation to IT or finance; forty-three per cent answerers from Chinese consumers show that they have an academic experience which is related to finance. Card users in China are having better qualified people in the field of finance/IT compared to India.

5.3.2 Correlation.

Table 2 represents the results of data analysis after SPSS was applied. We observed different findings after conducting the tests on the data received. Out of the 10-hypothesis produced 4 were significant for the Indian consumers while only one hypothesis could be accepted for the Chinese consumers. The correlation and significant value of all hypotheses are examined in table 2.

H1. The occurrence of internet frauds is associated with different age groups.

The data set collected by both countries could not support H1. In INDIA 41-50 age group (31.6%) has the greatest possibility of getting conned by fraudsters. In Chinese data collection there was no respondent. In all,

Analysis of financial frauds in electronic payment systems in India and China

52.1 per cent of the respondents were younger than 31 years old and 37.3 per cent fell into the age group 31-40 years old. The data showed us that majority of users from the Chinese mainland were young in age (21-30 years) and early middle-aged (31-40 years) people.

H2. The frauds which occur on the internet is associated with gender difference.

The results obtained from the Indian data set showed us that the Indian males were more susceptible to fall for fraudulent online transaction than females (i.e., about sixty-two per cent male to about thirty-eight per cent female). There was a crime report published in 2006 in the USA which suggested that males have higher chances to fall in the fraudsters trap than females and this report is consistent with the findings of that paper. H2 was rejected as it was observed in the data users of both countries that the required proportion of individuals being affected by fraudsters.

H3. The frauds which occur on the internet is associated with the difference in education levels.

People possessing qualification like BSc/BA/Prof in the Indian data group were found to be more susceptible to fraud and the proportion did not represent huge change although being most numerous in all the lots. There is no doubt that the education level of Chinese individuals is significantly lower when compared to western counterpart, but the data set gives us the idea that individuals who are highly educated in Chinese society have greater accessibility to the internet and therefore are more susceptible to frauds than the uneducated lot who are unlikely to use the internet.

H4. The frauds which occur on the internet is associated with bank card usage.

H4 was rejected Chinese and Indian data sets were compared, and financial organization would find this result in their favor and these results will help them persuade more people to use bank cards for any transactions done online.

Table 2. Correlation and significance value

Variables	INDIA			China Significance value		
	Correlation	Significance value	Hypo	Correlation	Significance value	Hypo
H1	-0.119	0.051	R	0.70	0.406	R
H2	-0.097	0.110	R	0.042	0.618	R
H3	0.105	0.083	R	0.074	0.382	R
H4	-0.022	-0.036	R	0.136	0.116	R
	0.745	0.561		0.100	0.239	
H5	0.211**	0.000	A	-0.055	0.518	R
H6	0.080	0.190	R	-0.019	0.812	R
H7	0.024	0.718	R	0.068	0.432	R
	-0.104	0.090		0.005	0.955	
H8	0.163**	0.007	A	0.046	0.590	R
H9	0.139*	0.023	A	0.040	0.639	R
	0.194**	0.001		-0.058	0.496	
H10	0.212**	0.000	A	0.165*	0.049	A
	0.124*	0.041		-0.048	0.572	R
	0.215**	0.000		-0.058	0.490	
	0.119*	0.050		0.020	0.815	
	0.210**	0.001		0.012	0.889	

H5. The frauds which occur on the internet is associated with usage of banking channels.

H5 is accepted as per responses received from the Indian citizens and it recommends that online banking is the sole medium which leads to fraud. (Tade, 2013) suggested that, about Rs.85 lakhs were lost to 150 Indian citizens who were victims of "419" in 2004. It is interesting to note that, the Chinese consumers, were not mentioned in any studies "419" frauds. Chinese data responses confirm that none of the respondents have faced

the “419” fraud and there is particular reason why they might not have been affected by it yet, the main reason being the language barrier. Studied by (Button, 2012), Malaysia where English was one of the official languages was the only country in the list which had the crime origin in their country. Customers in China who received a mail in English always thinks it as an error from the company side and directly ignore those kinds of emails.

H6. The frauds which occur on the internet is associated with the accounting management.

H6 had to be rejected based on the responses of the citizens of both the countries and these results will act as a booster for those companies who had been trying to convince customers to use the chip and pin technology willingly.

H7. The frauds which occur on the internet is associated with the customer’s satisfaction.

H7 was rejected based on the results but it was interesting to observe that the satisfaction level of both the countries were different as suggested by the responses from both countries. Out of the 7 fraud cases 5 fraud cases respondents said they were moderately satisfied with the bank responses and they scored them average and below average. 2 out of the 7 respondents did get their money from the bank, however they were not satisfied with the responses from their financial institutions mainly because of all the trouble they had to go through to get their money back from these banks. When we compare the Chinese data set with the Indian data set it was interesting to observe that the Indian customers who were defrauded were more satisfied with the bank’s responses compared to their Chinese counterparts.

H8. The frauds which occur on the internet is associated with the difference in the IT skills of individuals.

The majority of respondents who suffered from fraud attacks in the Indian subcontinent were people who believed that their IT skills was on an average level. We can use different ways to make a comparison between fraud occurrences experienced by consumers and their IT skill level. The first possible explanation is, the customer’s responses of their confidence in IT skills were purely based on the confidence of consumers. So, there is a high possibility that some respondents think very high of themselves, which might not be the actual case. A second explanation could be that we cannot and should not blame IT knowledge and IT infrastructure for every fraudulent transaction happening around the world. There is also a possibility that many fraudulent transaction take places because consumers were careless during their online transaction and it is also possible that the fraudster had intent to harm the consumer. For example, Reporting time of lost stolen cards is too late at times for the bank to take any action; Online customers reply to phishing emails with their information despite many warning by the banks and the government; Cashiers often record the card details and then they are traded to fraudsters in the black market. The third possible justification is that Consumers are more likely to be a part of online transactions if they are familiar with the online interfaces of various platforms and have significant IT skills and thereby are more likely to fall for fraudsters scams. A Study was conducted in a small IT sized company in INDIA and it was that most of them had experienced financial frauds on the internet and it was more common than we would like to think. Most of the respondents of the IT company were graduates and had the computer science degree.

H8 did not have much importance in the Chinese responses (7 of 143) and the reason for this could be that the majority of the Chinese respondents were less skilled in IT and hence had lesser probability to use online transactions.

H9. The frauds which occur on the internet is associated with IT usage frequency.

responses from both countries showed the confidence they had with respect to their IT skills. H9 had support from the Indian data as people here believed that the chances of them falling for a fraud were high since they were online more amount of time and likely to use the internet for the payments. The most important reason is the browser weakness which will be explained below.

The networking activities done nowadays is done on web browsers. Hence it should not be a surprise that it is being targeted by many fraudsters. In June 2000, Nike.com website was hacked, and consumers who tried to access <http://www.nike.com> in their browsers were redirected to a network in Scotland which was operated as a

team of hackers who identified themselves as S-11 and the host was FirstNet On-line Ltd. The Chinese dataset, for H9 did not show promising results as the responses received from China were very few in number. When people working in the industry were contacted in China, they said the banking system was aware of the frauds happening online worldwide and were taking steps to improve their security. One of the IT professionals working for one of the banks said that his bank has made a specialized team who only deals with the attack from the fraudsters be it hardware or software attacks.

H10. The frauds which occur on the internet is associated with online activity.

To make the survey questionnaire a draft of 5 questions were prepared which was 5 different activities: shopping in online websites, web browsing, Internet banking, online communication and media downloading. In the Indian data set, there was a strong relationship between consumers using the internet for various online activities and they being victims of fraud. However, it was seen that the Chinese consumers fell to fraud traps only if they were shopping online. There is a significant difference of online payment process in both the countries. When we compare Chinese regulations with Western countries, Chinese people have been experiencing online services for the very first time and managing finances at personal level, but also or more importantly, it is a condition that has to be met before which a person in China cannot access the internet for online transactions. The common way through which we Indian customers and the western world makes payment for transactions is that we submit details regarding consumers name, the card number and expiry date etc., at the website of the merchant directly. Indian Customers can do online shopping without using services from the bank that are online. Chinese consumers shopping experience in online mode is a complex in the sense that there is involvement of online services from banks right from the beginning of any transactions. But it can be said that due to this involvement there is additional security to consumers during online shopping. Chinese banks are trying to make the process of online shopping less complex, especially if the transaction is of a very small amount. Our learning from the earlier interviews from China that processes like OTP, instant alerts have become famous in the Chinese subcontinent as it takes care of the interest of consumers who are doing online shopping as well as offline.

5.3.3 Other interesting findings.

Apart from significance and correlation which have been discussed previously a few more tests were done and the findings are represented by Table 3, like the total number of cards and the satisfaction level of consumers in using these cards. As per the responses from the Indian consumers that people are more likely to have debit cards than credit cards. As per the data collected in INDIA, the respondents who are in possession of more debit cards will possibly have credit cards and related viewpoints were gathered from the Chinese consumers

Table 3. Customer’s responses findings

<i>Variables</i>	<i>INDIA</i>		<i>China</i>	
	<i>Correlation</i>	<i>Significance value</i>	<i>Correlation</i>	<i>Significance value</i>
Satisfaction with credit card service and history of credit card usage	0.142*	0.035	0.276**	0.001
Number of credit cards & number of debit cards	0.233**	0.000	0.257**	0.002
Satisfaction with credit card service and satisfaction with debit card service	0.623**	0.000	0.367**	0.000
History of branch banking channels usage and history of telephone banking channels usage	—0.055	0.370	0.166*	0.048
Prefer simple password/pin to complicated one and tend to use the same password/pin	0.365**	0.000	0.438**	0.000

Data Analysis

Payment policies in China can be the main reason for such high volumes of bank card possessions by consumers. When a Chinese bank customer wants to use a credit card the bank forces them to open a savings/salary account so that their debit card can be linked to the credit card so that when the transaction process is done it can be completed without any hurdles from the bank. Repayment methods for credit card dues in China are extremely less, so Chinese consumers usually agree to the bank's advice and open a savings/salary account and link it with their debit card to avoid hassles for repayment later. The only other option opens to Chinese bank customers is to carry cash to the bank at the end of the designated cycle and repay the credit card dues, but this is a very inconvenient procedure and the last option is to do fund transfers between the bank account but the processing fees for such a service is very high. The bank card service has been booming in China, but it is still in an initial phase and the banks are using this opportunity to make as much profits as possible by charging exorbitant service charge prices. As per the report by (Sina-Finance, 2010), the high service charge rates have been hindering banks growth in service cards segment and after a long debate in the country the prices were lowered in all financial organizations in China.

Limitations

The results from this research suggests that there are a number of areas where we can do research in the future, especially in the area of fraud as the area is quite under researched. Instead of asking bank consumers how they deal with fraud it would be much more insightful if we could ask a group of bank employees or the employees of other financial institutions as they deal with fraud on a daily basis. It would be interesting to analyze the various information for a researcher if we could somehow get past this level of secrecy maintained by the government of China. Hopefully in the future the author of the article can conduct such type of research and if the research could span international borders, there could be many more interesting things to be found out. It would be interesting to research different financial models of banks and the various assumption's banks make while classifying a case as fraud. There is very less chance of getting this research done as data required for this will be extremely confidential. There has been a worldwide increase in Mobile-commerce and shopping (Mallat, 2007). It would be an interesting research to conduct the behaviors of individuals in online shopping in the e environment and the mobile environment.

Conclusions

Banking service has been made quite efficient, and it has provided great convenience to consumers of online banking services who use for financial transactions. It is interesting to see that the Internet which is the primary survey for online transaction is also used extensively by fraudsters which makes the government and the people around the world lose billions of dollars every year ((Clemes et al., 2014);(Xiao & Benbasat, 2011)). This study helps us understand the attitude of consumers towards online services provided by banks and fraud occurrences internationally. The data from this study can be used in the future by various local bodies and governments to enlighten their citizens of various type of fraud and how they fall prey to these fraudsters. This activity would help both financial institutions and consumers. Educating customers in both countries regarding the ways in which these fraudsters operate is going to be very beneficial. As per the analyses and the collection process of various data we can say that consumers are well informed of banking policies and certain type of frauds to an extent. Especially in China, the contentedness of consumers is relatively low when compared to Indian consumers and the service quality is below acceptable limits in most circumstances. Two methods are possible to reduce financial frauds with the help of educating consumers to limit details shared that are very personal on the internet and to identify places where deception is likely to happen. Firstly, to understand consumer behaviors we have to understand self-disclosure on the internet and link various attitude of consumers and behaviors can be indicated efficiently (Joinson et al., 2010) and (Schiffrin et al., n.d.). Secondly, consumers should have enough materials to identify the cases that can lead to deception, most of times they are old ploy but camouflaged by new medium – Cyberspace (Wright et al., 2010) and (Mavlanova & Benbunan-Fich, 2010).

References

- [1] Agarwal, R., Rastogi, S., & Mehrotra, A. (2009). Customers' perspectives regarding e-banking in an emerging economy. *Journal of Retailing and Consumer Services*, 16(5), 340–351. <https://doi.org/10.1016/j.jretconser.2009.03.002>
- [2] Black, N. J., Lockett, A., Winklhofer, H., & Ennew, C. (n.d.). (Early draft of the paper finally published in *Int Jnl of Retail and Distribution Management*) The Adoption of Internet Financial Services: A Qualitative Study.
- [3] Button, M. (2012). Cross-border fraud and the case for an “Interfraud.” In *Policing* (Vol. 35, Issue 2, pp. 285–303). <https://doi.org/10.1108/13639511211230057>
- [4] Buzzetto-Hollywood, N. (2014). Management in a Web 2.0 World: Risks and Counter-Measures E-Portfolios View project Grit in Higher Education View project. <https://www.researchgate.net/publication/228969971>
- [5] Casu, Barbara., Molyneux, Philip., & Girardone, Claudia. (2006). *Introduction to banking*. Prentice Hall Financial Times.
- [6] Clemes, M. D., Gan, C., & Zhang, J. (2014). An empirical analysis of online shopping adoption in Beijing, China. *Journal of Retailing and Consumer Services*, 21(3), 364–375. <https://doi.org/10.1016/j.jretconser.2013.08.003>
- [7] davis1989. (n.d.).
- [8] Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet (Vol. 13).
- [9] Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of Internet banking adoption. In *Telematics and Informatics* (Vol. 31, Issue 3, pp. 492–510). <https://doi.org/10.1016/j.tele.2013.04.003>
- [10] Hoehle, H., Scornavacca, E., & Huff, S. (2012). Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis. *Decision Support Systems*, 54(1), 122–132. <https://doi.org/10.1016/j.dss.2012.04.010>
- [11] Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31(2), 177–192. <https://doi.org/10.1002/ejsp.36>
- [12] Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1), 1–24. <https://doi.org/10.1080/07370020903586662>
- [13] Lin, H. Y., & Hsu, C. L. (2011). A novel identity-based key-insulated convertible authenticated encryption scheme. *International Journal of Foundations of Computer Science*, 22(3), 739–756. <https://doi.org/10.1142/S0129054111008325>
- [14] Logsdon, J. M., & Patterson, K. D. W. (2009). Deception in Business Networks: Is It Easier to Lie Online? *Journal of Business Ethics*, 90(SUPPL. 4), 537–549. <https://doi.org/10.1007/s10551-010-0605-z>
- [15] Mäenpää, K., Kale, S. H., Kuusela, H., & Mesiranta, N. (2008). Consumer perceptions of Internet banking in Finland: The moderating role of familiarity. *Journal of Retailing and Consumer Services*, 15(4), 266–276. <https://doi.org/10.1016/j.jretconser.2007.05.007>
- [16] Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1), 1–13. <https://doi.org/10.1016/j.ijinfomgt.2013.06.002>
- [17] Mavlanova, T., & Benbunan-Fich, R. (2010). Counterfeit products on the internet: The role of seller-level and product-level information. *International Journal of Electronic Commerce*, 15(2), 79–104. <https://doi.org/10.2753/JEC1086-4415150203>
- [18] Mckechnie, S. (1992). Consumer Buying Behaviour in Financial Services: An Overview. *INTERNATIONAL JOURNAL OF BANK MARKETING*, 10(5), 4–12.
- [19] McKenna, K. Y. A., & Green, A. S. (2002). Virtual group dynamics. In *Group Dynamics* (Vol. 6, Issue 1, pp. 116–127). American Psychological Association Inc. <https://doi.org/10.1037/1089-2699.6.1.116>
- [20] Nasri, W., & Charfeddine, L. (2012). Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior. *Journal of High Technology Management Research*, 23(1), 1–14. <https://doi.org/10.1016/j.hitech.2012.03.001>
- [21] Nguyen, M., Bin, Y. S., & Campbell, A. (2012a). Comparing online and offline self-disclosure: A systematic review. In *Cyberpsychology, Behavior, and Social Networking* (Vol. 15, Issue 2, pp. 103–111). <https://doi.org/10.1089/cyber.2011.0277>

- [22] Nguyen, M., Bin, Y. S., & Campbell, A. (2012b). Comparing online and offline self-disclosure: A systematic review. In *Cyberpsychology, Behavior, and Social Networking* (Vol. 15, Issue 2, pp. 103–111). <https://doi.org/10.1089/cyber.2011.0277>
- [23] Pol, L. G. (1986). *MARKETING AND THE DEMOGRAPHIC PERSPECTIVE*.
- [24] Powers, T. L., & Sterling, J. U. (2008). Segmenting business-to-business markets: A micro-macro linking methodology. *Journal of Business and Industrial Marketing*, 23(3), 170–177. <https://doi.org/10.1108/08858620810858436>
- [25] Qi, M., Carbó-Valverde, S., & Rodríguez-Fernández, F. (2016). The diffusion pattern of non-cash payments: Evidence from China. *International Journal of Technology Management*, 70(1), 44–57. <https://doi.org/10.1504/IJTM.2016.074652>
- [26] Quazi, A., & Talukder, M. (2011). Demographic determinants of adoption of technological innovation. *Journal of Computer Information Systems*, 51(3), 38–46. <https://doi.org/10.1080/08874417.2011.11645484>
- [27] Rogers, D. (1986). Demographic data reports How they can be used by retailers *DEMOGRAPHIC DATA*.
- [28] Rogers, E. M., Singhal, A., & Quinlan, M. M. (2019). Diffusion of innovations. In *An Integrated Approach to Communication Theory and Research*, Third Edition (pp. 415–433). Taylor and Francis. <https://doi.org/10.4324/97802037110753-35>
- [29] Rotchanakitumnuai, S., & Speece, M. (2003). Barriers to Internet banking adoption: A qualitative study among corporate customers in Thailand. *International Journal of Bank Marketing*, 21, 312–323. <https://doi.org/10.1108/02652320310498465>
- [30] Schiffrin, H., Edelman, A., Falkenstern, M., & Stewart, C. (n.d.). The Associations among Computer-Mediated Communication, Relationships, and Well-being.
- [31] Sina-Finance. (2010). CPPCC National Committee member. http://finance.sina.com.cn/money/bank/bank_hydt/20110304/07109470268.shtml
- [32] Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The “yahoo plus” phenomenon. *Human Affairs*, 23(4), 689–705. <https://doi.org/10.2478/s13374-013-0158-9>
- [33] Tsai, C. L., Chen, C. J., & Zhuang, D. J. (2012). Secure OTP and biometric verification scheme for mobile banking. *Proceedings - 2012 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, MUSIC 2012*, 138–141. <https://doi.org/10.1109/MUSIC.2012.31>
- [34] Tzeng, S.-F., Hwang, M.-S., & Chen, H.-B. (2005). A secure on-line software transaction scheme. *Computer Standards & Interfaces*, 27(3), 303–312. <https://doi.org/10.1016/j.csi.2004.07.004>
- [35] Vincent, O. R., Folorunso, O., & Akinde, A. D. (2010). Improving e-payment security using Elliptic Curve Cryptosystem. *Electronic Commerce Research*, 10(1), 27–41. <https://doi.org/10.1007/s10660-010-9047-z>
- [36] Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? understanding the deception in phishing communications. *Group Decision and Negotiation*, 19(4), 391–416. <https://doi.org/10.1007/s10726-009-9167-9>
- [37] Xiao, B., & Benbasat, I. (2011). Product-Related Deception in E-Commerce: A Theoretical Perspective A Theoretical Perspective1. In *Source: MIS Quarterly* (Vol. 35, Issue 1).