International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournal.com

© **Serials Publications Pvt. Ltd.**

Volume 15 • Number 21 • 2017

A Study on Impact of Collectivism Amongst Floating Population in Bengaluru, Karnataka on ATM Identity Theft

S. Divya Meena[1], Cherian Thomas[2] and N. Sundaram[3]

[1]*Research Scholar, School of Information Technology and Engineering, VIT University, Vellore- 632 014, Tamil Nadu, India. Email: sdivya.meena2017@vitstudent.ac.in*

[2]*Research Scholar, Department of Commerce, School of Social Sciences and Languages, VIT University, Vellore 632 014, Tamil Nadu, India. Email: cherian28@gmail.com*

[3]*Professor and Head, Department of Commerce, School of Social Sciences and Languages, VIT University, Vellore 632 014, Tamil Nadu, India. Email: nsundaram@vit.ac.in*

ABSTRACT

In a world where houses, electronic devices, bank and social media accounts, vehicles, lockers etc., are controlled by passwords, identity theft looms large in case of bank accounts too. Through skimming and other cyber frauds, scamsters are able to steal money as well as compromise with customer's passwords and identity. Once a person's identity is compromised, the same might be used elsewhere anonymously to run transactions. This puts bank customers into quandary. Such a cyber crime is hard to trace out and developing countries lack enough infrastructures to do so. The sample size for the study was 400 floating population of Bengaluru. The analysis was done using simple random sampling and a three point Likert scale. A pilot study was conducted with 10 respondents before finalizing the questionnaire. Cronbach's Alpha was used to test the reliability of the data. Pearson's Chi Square Test of Association was used to find the association between demographic and inferential variables. Pearson's Chi Square Test of Independence was used to measure the impact that independent variables had on dependent variables. This paper is a study towards the Collectivism behavior that exists in Indian society, which could possibly lead to damage and misuse of bank customer's identity through the usage of Automated Teller Machines (ATM).

Keywords: ATM, Identity theft, Collectivism, Bengaluru.

1. INTRODUCTION

Collectivism is defined differently across spheres like political ideology and philosophy. In this study, collectivism is placed in the context of culture. It is referred as placing a groups' interest over and above an

individuals' interest. Each individual is accountable for others' actions. There are two types of Collectivism viz. horizontal and vertical collectivism. Horizontal collectivism focuses on a group. The groups' ideals are held high than individual ideals. Vertical collectivism on the other hand focuses on the hierarchy. It is the authority's ideals to which people surrender. In this study, horizontal collectivism alone has been focused. Collectivism as a culture evolved in India, which promoted joint family system, at the micro level and in a macro level, it was seen in family run businesses like Joint Hindu Family system. As time passed, nuclear family system had started gaining ground in urban cities of India and it is paving way to disintegration of Collectivism. An article in Quartz India by J. S Raja (2014), testifies by comparing 2001 and 2011 Indian Census, that there has been shift towards growth in nuclear families, but the rate of change is still low. As per Modernization theory, industrialization and urbanization is supposed to speed up the rate of nuclear families, but it has not happened so far in India. Hence, one can say that the culture of Collectivism has not disappeared.

Floating population is an expression given to those set of people, in a given area, that do not reside more than five years and vacate as soon as their task or education is completed. They do not come under the purview of electoral list and nor are they taken into account during the census survey. As cites grow migration increases and this gives way to floating population. The reason for such a migration was mainly due to the need for a job or education. A new place creates unfamiliarity in the mind of migrants. This is where collectivism comes to play. Bengaluru district in Karnataka was taken as the place of study because of its' richly diverse population. Expatriates as well as people from different states of India add up to ten lakhs as per 2011 Census Survey of India. The ability of the city to garner venture capital funds worth 3,014 crores in 2013, as per Venture Intelligence, indicates about the places' robust eco –system to house more startups and provide new employment opportunities.

Financial identity theft refers to utilizing customers' bank account details to conduct financial crime through skimming, shoulder surfing or misusing someone's obtained ATM password. It adds up to seventy seven percentage of cyber crimes that happens in India as per Experian's Fraud Report (2016). The report also states that credit cards are more prone to identity theft than debit cards. Javelin Strategy & Research's report called year 2016 as the year of identity theft, by analyzing the alarming rise of identity thefts that happened globally. The Reserve Bank of India has received reports from banks about 11,997 cases related to ATM, and Net banking frauds in 2015-16. Indian Computer Emergency Response Team (CERT-In) puts the number higher at 49,455 cyber security incidents, in 2015. These figures do not take into account such incidents that go unreported. Identity theft is akin to an epidemic and it can be controlled by proper preventive measures. One of the measures is to refrain from sharing information and also shredding sensitive information like passwords.

The study proposes a model to study this identity theft, in the context of ATM users. Figure 1.1 gives a brief outline of it.

The above given model was framed using the following variables given under each heading. The variables were shortened for easier naming. The meaning of each variable is mentioned below:

(a) Dependence:

(i) *Operation of Card:* It explains about the help that an individual takes from others in order to withdraw money from ATM.

(ii) *Reason to depend:* This variable investigates the necessity behind seeking dependence.

(iii) *Dependence on dependent:* This variable focused on the individual's dependents who would act as a resort in times of crisis.

(iv) *Situations depended:* It asks the respondents to recall any past event that were critical or self manageable, before seeking dependence.

(v) *Dependence due to no plans:* The respondents were asked to evaluate if dependence came in to play due to negligence shown in planning finances

(b) Security

(i) *Password reset:* The respondents were asked to recall as to how long it has been since their last ATM Pin change.

(ii) *Going cashless:* Given an option, whether the respondents were able to use cashless options and avoid an ATM Transaction.

(iii) *Account balance check:* The respondents were asked to evaluate if they would periodically check the account transactions that were occurring in their bank accounts.

(iv) *Card operation by third party:* The frequency of a third party using an individual's ATM card was measured.

(v) *Assurance:* After sharing the password of the ATM Card does the individual take any resolutions to never share the password with anyone.

(c) Trust:

(i) *Suspecting:* This variable was used to see what weighed more for an individual, whether it was trust or suspicion.

(ii) *Known deception:* It was checked if the individual was familiar with a third party card user

(d) Awareness

(i) *Cyber fraud awareness:* The awareness level about cyber attacks happening around was checked.

(ii) *Dependent's knowledge:* This variable checked if the dependents of individuals were aware about their password sharing activity with a stranger.

(iii) *Bank's awareness effort:* The individual was asked to rate bank's efforts to make him or her aware of cyber frauds and preventive measures that needs to be taken.

(e) Culture

(i) *Money withdrawal offer:* On the threshold of collectivism, the individual was asked to evaluate as to how he or she viewed a third party's offering to withdraw money on their behalf.

(ii) *Culture learning:* The source of learning collectivistic culture was questioned.

(iii) *Withdrawal decision:* The amount to be withdrawn from an ATM vests in the hands of the individual or a third party.

The objectives of the study are as follows:

- To measure the impact of collectivism characteristics on identity theft of ATM users
- To understand the cyber fraud awareness amongst floating population
- To study the cultural influence towards endless collectivism in India

Based on the objectives, eight hypotheses were set.

2. REVIEW OF LITERATURE

The term 'culture' is referred to as a combination of a person's traditions, religious systems, personal, influenced and handed over values and beliefs. Culture changes over time and this is reflected in the article of Kshetri (2016). The author affirms that culture plays a vital role in cyber crimes that happen and people are bound to have a sense of sharing passwords and facing identity theft due to the culture that surrounds them. It is for this reason that Gilbert (2014) calls upon cyber security experts to study human behavior, since behavior and cyber crimes are closely related. More number of studies has focused on a factor known as 'Trust', which is a part of culture itself. Ntuen et. al., (2014) draws an inverse relationship between trust and cyber risk that is noticed in people. The article states that a high trust is a result of lesser risk. To heighten trust, cyber risk must reduce. Reddy (2016) opines that even if norms are in place, unless ethical values are set right, we are not going to find a credible solution for this.

Education is a powerful tool to change human minds. Ogoh (2016)'s thesis re-affirms it and advocates for a universal awareness about such a problem. Nathan et. al., (2016) views cyber frauds as a major opportunity to get people aware and ready. It is seen as an opportunity since there is a threat present to one's own financial security. The onus has not only been set on people alone, and indeed it is set on banks as well. Sanusi et. al., (2015) specifically refers to senior management of banks to be propagators of cyber safety amongst employees. Moreover, as time passes, a bank needs to learn from cyber security lapses that had occurred previously. Such an onus is seen vital since there is loss for people as well as banks. This study specifically focuses on peoples' loss and that is pointed out by Gupta et. al., (2015), in which loss is divided as both physical as well as mental. On the physical side is the loss of cash and on the mental side is the loss of confidential identity information. As far as banks are concerned, they stand to lose integrity as per Edwin (2014). Taiwo et. al., (2016) views it in broader perspective. They state that bank's integrity takes a hit on the economy since such affected banks will have insufficient cash to lend for potential borrowers. Even if the loss mentioned is huge, both people as well as banks still seem complacent. Romanosky (2016) brings this to light by stating that banks view cyber attacks as minimal loss and hence invests meagerly towards cyber security measures. Several solutions intended to combat cyber crimes have hit road block due to the quandary that is surrounding the nature of banking transactions. Chesang (2016) brings joint account transactions and refers to the lack of security seen in issuing a common ATM Personal Identification Number to both the individuals. In the same way, Zulhuda (2015) advocates to make Sharia Law relevant to the present era, since identity theft is not recognized by law. Forgery and fraud are considered to be unlawful; hence even identity theft has to be brought inside the purview.

Chen and Chou (2014) made a pitch for future technology to separate customer's identity information from the transactions that are undertaken. Thereby the authors have asked to overturn the very nature

of how cashless transactions are being done. This would not put identity of any individual at stake. In a recent ATM fraud in India, which affected 3.2 lakhs of bank customers on 20th September, 2016, one of the affected banks, resorted to re-issue of cards. This option whether decided beforehand or taken in haste was seen as an ineffective and temporary measure to this problem according to Graves et. al., (2015). The trying part of such a mess is when no one owns up such frauds and the customer is left in the lurch due to the untraceable activity of scamsters. Dzomira (2015) attributes it to the disconnected environment of the banking domain in developing countries. The author highlights the need for a connected environment which involves individuals, merchants, government, business entities and public institutions in order to make e-risk management effective, so that any cyber fraud is the shared responsibility of all the stakeholders. Creation of connected environment does not solve the problem as per Mas and Porteous (2015). This is because of the difference in how an individual's identity is handled between different stake holders. It creates identity security gaps. Unless these gaps are plugged in, one cannot put an end to this crisis. At the micro-level, Riley (2015), paints a stark reality which tells that forty three percent of identity theft are committed by family members and victim's known acquaintances. Be it known individuals or organizations, who rob customers' identity, Broadhurst et. al., (2014) admits that these scamsters tend to be skilled and well armed to carry out such attacks. The problem with dealing with ATM frauds is, it is expensive in nature. Reserve Bank of India had issued a directive to all banks to switch to replace all magnetic strips plastic cards with EMV (Europay, Master and VISA) chip and pin, in order to prevent skimming from September 2015, it will create another financial burden for undergoing such a massive change. Moreover, such a move is a temporary solution, since it does not stop the financial spur that scamsters will receive from committing such acts as per Sullivan (2015). It calls for an even more in depth micro study to analyze peoples' attitude in order to have a broader plan in place, because no matter whatever security protocols are in place, scamsters will come up with ideas to infiltrate it.

From the previous studies, it was found that micro and macro studies were conducted on ATM identity theft, over the years. The pros and cons, the accountability, the environment, sources and stakeholders have been brought to light. Lack of awareness is the often used word, which is focused on majority of studies. Going even more in depth into the culture of an individual, that is still keeping individuals prone to identity theft attacks, a study by Riley et. al., (2015) strikes very close to this study. Kshetri (2016) too has given collectivism as an example to changing culture and it's implication on individuals. This study takes up collectivism in the Indian background and further studies it with the floating population, thereby taking collectivism studies one step ahead by not only taking changing time and culture but changing population as well into account.

3. RESEARCH METHODOLOGY

The sample size was selected as 400 by using Godden, 2004's formula for infinite population. The analysis was done using simple random sampling. A three point Likert scale was used in building the questionnaire. A pilot study was conducted with 10 respondents before finalizing the questionnaire. Cronbach's Alpha was used to test the reliability of the data. Pearson's Chi Square Test of Association was used to find the association between demographic and inferential variables. Pearson's Chi Square Test of Independence was used to measure the impact that independent variables had on dependent variables.

4. RESULTS AND DISCUSSION

The reliability of the data was tested using Cronbach's Alpha and it was found to have 0.870, which shows a high reliability (Table 1).

Table 1
Cronbach Alpha's Reliability Test

Cronbach's Alpha	*N of Items*
0.870	24

The Normality Test was tested using Shapiro Wilk Test and it was found out that all the hypotheses in the data were having a *p* value of 0.000 and hence the data was not normally distributed. This led the study to be conducted using Non-parametric test. Hence, Chi-square test was used to test all the hypotheses.

The Chi-square Test of Association was carried out to check the variation in opinions generated across various strata of the society. It was found that there was no statistically significant association between demographic variables and inferential variables since $p > 0.05$. The respondents were found to have no difference of opinion based on the various strata that they belonged.

A summary of the respondent's demographic variable showed that 56% of the respondents were male. 40% of the respondents came under the age range between 41 and 50. 31% of the respondents were graduates. 38% of the respondents stayed in the urban area.

37% of the respondents worked in the private sector and 39% of them earned an income between ₹15,001 and ₹30,000.

The Chi-square Test of Independence was used to test all the hypotheses.

$H_0$1: Money withdrawal offer has no impact on dependence on dependent.

Table 2
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	2.319	4	0.677

$H_0$1 had no significance, since *p* value was greater than 0.05. The null hypothesis was accepted. It means that money withdrawal offer had no impact on dependence on dependent.

$H_0$2: Culture learning has no impact on known deception.

Table 3
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	351. 220	2	0.000

$H_0$2 had significance, since *p* value was lesser than 0.05. The null hypothesis was not accepted. It means that culture learning had an impact on known deception.

$H_0$3: Educational qualification has no impact on cyber fraud awareness.

Table 4
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	9.875	3	0.020

$H_0$3 had significance, since *p* value was lesser than 0.05. The null hypothesis was not accepted. It means that educational qualification had an impact on cyber fraud awareness.

$H_0$4: Area of residence has no impact on dependent's knowledge.

Table 5
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	0.036	2	0.982

$H_0$4 had no significance, since *p* value was greater than 0.05. The null hypothesis was accepted. It means that area of residence had no impact on dependent's knowledge.

$H_0$5: Bank's awareness effort has no impact on password reset.

Table 6
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	80.471	3	0.000

$H_0$5 had significance, since *p* value was lesser than 0.05. The null hypothesis was not accepted. It means that bank's awareness effort had an impact on password reset.

$H_0$6: Employment type has no impact on going cashless.

Table 7
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	1.890	3	0.596

$H_0$6 had no significance, since p value was greater than 0.05. The null hypothesis was accepted. It means that employment type had no impact on going cashless.

$H_0$7: Age has no impact on withdrawal decision.

Table 8
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	1.097	3	0.778

$H_0$7 had no significance, since *p* value was greater than 0.05. The null hypothesis was accepted. It means that age had no impact on withdrawal decision.

$H_0$8: Suspecting has no impact on card operation by third party.

Table 9
Chi-Square Tests

	Value	*Df*	*Asymp. Sig. (2-sided)*
Pearson Chi-Square	273.512	4	0.000

$H_0$8 had significance, since *p* value was lesser than 0.05. The null hypothesis was not accepted. It means that suspecting had an impact on withdrawal decision.

5. CONCLUSION, LIMITATION AND SCOPE FOR FURTHER RESEARCH

Based on the objectives that this study was undertaken, few of the factors showed significance and few others were not significant. It was analyzed as follows: The impact of collectivism characteristics on identity theft of ATM users was tested and found out that collectivism culture was thrust upon by family upon an individual and it is this factor that urges individuals to share their password without hesitation to their known family members with ease. The source of password sharing and the risk prone area of identity theft were pointed at the family itself. On the attitude that was formed as part of this, it was found that it was less likely for the individuals to reach out to strangers who are unknown even if the collectivism character was stronger in them.

The second objective was aimed at understanding if there was an awareness amongst floating population about the cyber frauds that were happening around them and their family's awareness about their own follies when they engaged in password sharing. The respondents were of the view that neither their job or the area from which they come from had anything to do with cyber fraud awareness. Such awareness was created mainly through education and in banks. The efforts taken by educational institutes and banks across urban and rural areas were placed with high appreciation.

The final objective was to study the cultural influence towards endless collectivism in India. No matter the age, seniority in a family did not bring individualism to the fore. Collectivism did persist. Trusting others was considered as a good virtue than suspicion and this would have triggered collectivism to never have an end even after the emergence of more nuclear families in India.

The study was conducted during a shorter time. The study is not based on any model.

Future studies could focus on specific regional culture rather than taking multi cultural, as seen in this study.

References

N. Blascak et. al., (2016), "Identity Theft as a Teachable Moment". Research Department, Federal Reserve Bank of Philadelphia, Working Paper 16-27, pp. 1-47.

P.I. Ogoh (2016), "The Role Management plays in Combating Cybercrime within Nigeria's Banking Industry". Diss. Colorado Technical University, pp. 1-44.

Z.M. Sanusi et. al., (2015), "Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss." Procedia Economics and Finance 28, pp. 107-113.

K.S. Reddy (2016),"Cyber Crimes in India and the Mechanism to Prevent them", International Journal of Innovative Research in Information Security, No. 3, Dec, pp. 29-32.

M.E Agwu (2014), "Reputational Risk Impact of Internal Frauds on Bank Customers in Nigeria." International Journal of Development and Management Review, 9.1, pp. 175-192.

E.K. Chesang et. al., (2016), "Implementing an SMS-based Authentication Framework for a Joint Account ATM Transaction." Mara Research Journal of Information Science and Technology, 1, pp. 134-144.

S. Zulhuda and S. Mohamed (2015), "The Shari'ah Approach to Criminalise Identity Theft." Pertanika Journal of Social Sciences & Humanities, 23 (S), pp. 169-182.

Y. Chen and J. Chou (2014), "ID-Based Certificateless Electronic Cash on Smart Card against Identity Theft and Financial Card Fraud." The International Conference on Digital Security and Forensics, The Society of Digital Information and Wireless Communication, pp. 57-67.

E. Victoria et. al., (2016), "Deploying ICT with Entrepreneurship Culture can Fight Cyber-Crime Menace in Developing Countries." West African Journal of Industrial and Academic Research, 16.1, pp. 58-67.

N. Kshetri (2016), "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future." Crime, Law and Social Change, 66.3, pp. 313-338.

J.A. Gilbert (2014), "Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours: An Application of the Theories of Planned Behaviour and Protection Motivation." Diss., McMaster University, pp. 1-280.

J.N. Taiwo et. al., (2016), "Growth of Bank Frauds and the Impact on the Nigerian banking Industry." Journal of Business Management and Economics, 4.12, pp. 1-10.

D. Riley et. al., "Identity Theft among American Indian and Alaskan Native Elders." National Indian Council on Aging, Inc., (2015), pp. 1-3.

R.J. Sullivan (2014), "Controlling Security Risk and Fraud in Payment Systems." Economic Review-Federal Reserve Bank of Kansas City, pp. 5-36.

C.A. Ntuen et. al., (2014), "Modeling the relationship between trust and risk in cyberspace." IIE Annual Conference Proceedings, Institute of Industrial Engineers, pp. 123-131.

P. Gupta and R.A. Mata-Toledo (2016), "Cybercrime: In Disguise Crimes." Journal of Information Systems & Operations Management, pp. 1-10.

J.T. Graves and et. al., (2014), "Should Payment Card Issuers Reissue Cards in Response to a Data Breach." Workshop on the Economics of Information Security, pp 1-31.

I. Mas and D. Porteous (2015), "Minding the Identity Gaps." Innovations, 10.1-2, pp. 27-52.

S. Romanosky (2016), "Examining the Costs and Causes of Cyber Incidents." Journal of Cybersecurity, pp. 121-135.

S. Dzomira (2014), "Cyber-banking fraud risk mitigation conceptual model." Banks and Bank Systems, 10, 2, pp. 7-14.

R. Broadhurst et. al., (2014), "An Analysis of the Nature of Groups Engaged in Cyber Crime.", International Journal of Cyber Criminology, pp. 1-26.