International Journal of Economic Research
Volume 15, Number 2, 2018, ISSN : 0972-9380
available at http: www.serialsjournals.com

PRODUCT VULNERABILITY IN INDIAN BANKING SECTOR

K. Sankara Moorthy[1] and G. Kumar[2]

[1] *Assistant Professor,SRM School of Management, Chennai*
[2] *Assistant Professor,SRM School of Management, Chennai*

Abstract: Technology is a double edged sword as it has its merits and demerits. Adoption of tech tools in the financial sector has transformed the banking industry and enhanced the convenience among the customers. Availability of smart phones has increased the accessibility of banking services in a click of a button. Despite the advantages, the medium becomes more vulnerable to hackers. This paper discusses the overview of nature of bank frauds in India.

Keywords: Challenges of Electronic banking , fraud detections, ATM frauds, credit card frauds, debit card frauds, net banking frauds

INTRODUCTION

The increased use of third party applications and technology has made the information of users in the Internet space vulnerable to hackers. Customers have reached a period where they cannot avoid the technology. Understanding the data of the bank frauds gives the idea in establishing policy decision in the part of the banks. Public image of the banks is important in coping up the tough competition in the banking sector. Security is one of the prime factor that helps in retaining a customer with the bank.

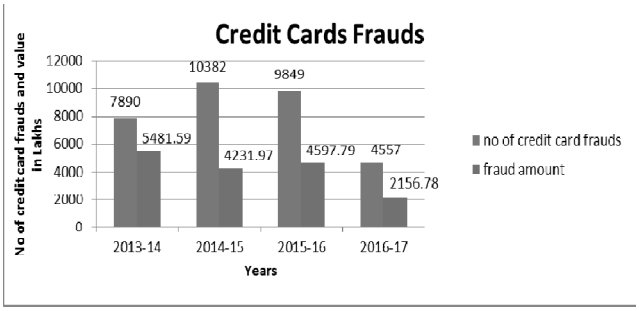
LITERATURE REVIEW

Awareness of customer, staff education, internal controls play a major role in prevention of fraud in electronic banking(Usman & Shah, 2013). Fraud detection tools, Fraud detection technology, cyber law , education is the important factor in prevention of electronic banking fraud(Dzomira, 2014). Biometric authentication system is most important one in preventing the fraud in the electronic banking system(Fatima, 2011). Trust generation is the important factor in the electronic banking system(Munoz Leiva, Luque Martínez, & Sanchez Fernández, 2010). Effective tools and techniques should be needed to prevent electronic banking fraud (Wei, Li, Cao, Ou, & Chen, 2013). Both customer and bank both responsible for prevention of fraud in the electronic banking system(Adepoju & Alhassan, 2010). Hidden Markov Model may be used to prevent fraud in the credit cards electronic banking system(Iyer, Mohanpurkar, Janardhan, Rathod, & Sardeshmukh, 2011). Cost, security perceived risk, quality of services play a major role in adoption of electronic banking system. (Taeb, 2012).

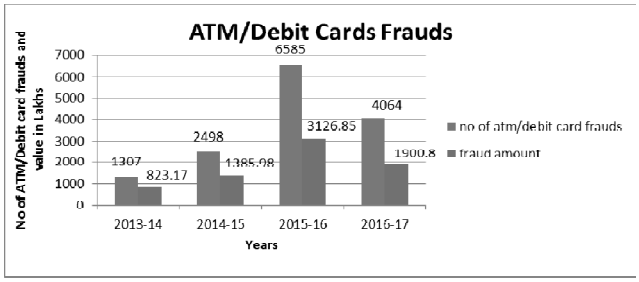
RESEARCH METHODOLOGY

Data is extracted from India stat data repository website and analyzed using MS Excel. Bar charts are used to understand the pictorial representation of the data.

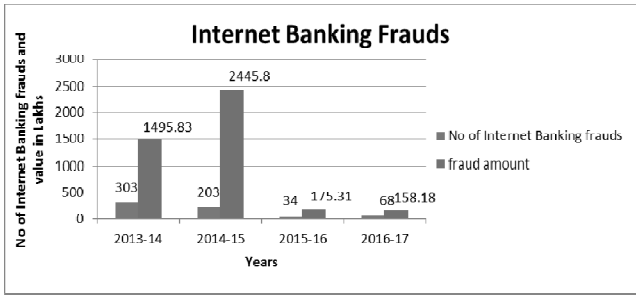
DATA ANALYSIS AND INTERPRETATION



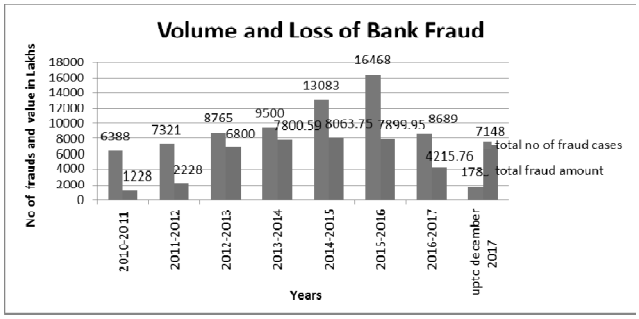
From the above chart ,we can infer that the number of credit cards fraud is declining while the fraud amount is not declining substantialy.



From the above chart, we can infer that the number of ATM Frauds was higher in the year 2015 – 2016 and it has reduced to 4064 cases in the year 2016-2017.



From the above chart, we could infer that the number of internet banking frauds have reduces to a greater extent due to the advanced security policies adopted by the bank, while there is a slight increase in the year 2016 – 2017.



From the above chart we could infer that the volume of bank frauds have decreased , while the loss remains almost the same.

CONCLUSION

We could understand that there is a increased risk on high value transactions and the accounts having higher amount of money. Banks have to concentrate on innovative technology tools to monitor the risk of the high value transactions.Awareness among the customers regarding the hacking methods and safety measures must be the prime step in controlling the bank frauds.

REFERENCES

Adepoju, A. S., & Alhassan, M. E. (2010). Challenges of Automated Teller Machine (ATM) usage and fraud occurrences in Nigeria - A case study of selected banks in Minna metropolis. Journal of Internet Banking and Commerce. 15(2),page no 1-10. https://doi.org/10.1007/978-3-531-92534-9_12

Dandash, O., Wang, Y., Le, P. D., & Srinivasan, B. (2008). Fraudulent internet banking payments prevention using dynamic key. Journal of Networks, 3(1), 25–34. https://doi.org/10.4304/jnw.3.1.25-34

De Luca, A., Langheinrich, M., & Hussmann, H. (2010). Towards understanding ATM security: a field study of real world ATM use. SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security, 1–10. https://doi.org/http://doi.acm.org/10.1145/1837110.1837131

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance and Control: Financial Markets and Institutions, 4(2), 16–26. *https://doi.org/10.22495/rgcv4i2art2*

Fatima, A. (2011). E-banking security issues-Is there a solution in biometrics? Journal of Internet Banking and Commerce, 16(2)

Ho, S. S. M., & Ng, V. T. F. (1994). Customers2 Risk Perceptions of Electronic Payment Systems. International Journal of Bank Marketing, 12(8), 26–38. https://doi.org/10.1108/02652329410069029

Iyer, D., Mohanpurkar, A., Janardhan, S., Rathod, D., & Sardeshmukh, A. (2011). Credit card fraud detection using Hidden Markov Model. 2011 World Congress on Information and Communication Technologies, 5, 1062–1066. https://doi.org/10.1109/WICT.2011.6141395

Khanna, A., & Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in indian banking industry. International Journal of Business Science and Applied Management, 4(3), 1–21.

Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, 8(3), 130–141. *https://doi.org/10.1016/j.elerap.2008.11.006*

Mahdi, M. O. S. (2011). Trust and security of electronic banking services in Saudi commercial banks: Saudis versus Non Saudis opinions. African Journal of Business Management, 5(14), 5524–5535. https://doi.org/10.5897/AJBM11.682

Munoz Leiva, Luque Martínez, & Sanchez Fernández,.(2010). How to improve trust toward electronic banking. Online Information Review, 34(6), 907–934. https://doi.org/10.1108/14684521011099405

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. Electronic Commerce Research and Applications, 19, 33–43. https://doi.org/10.1016/j.elerap.2016.07.001

Taeb, R. (2012). Adoption of Electronic Payment Services by Iranian Customers. Successful Customer Relationship Management Programs and Technologies, 1(December), 268–285. https://doi.org/10.4018/978-1-4666-0288-5.ch018

Tripathi, K. K., & Pavaskar, M. A. (2012). Survey on Credit Card Fraud Detection Methods. International Journal of Emerging Technology and Advanced Engineering, 2(11), 721. https://doi.org/10.18535/Ijecs/v4i11.25

Usman, A. K., & Shah, M. H. (2013). Critical success factors for preventing E-banking fraud. Journal of Internet Banking and Commerce, 18(2). https://doi.org/10.1007/978-3-531-92534-9_12

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web, 16(4), 449–475. *https://doi.org/10.1007/s11280-012-0178-0*

Zareapoor, M., Seeja.K.R, S. K. ., & Afshar Alam, M. (2012). Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria. International Journal of Computer Applications, 52(3), 35–42. *https://doi.org/10.5120/8184-1538*