Global Management Review
Vol 14, Issue 2, July - December 2020

A STUDY ON UNAUTHORISED TRANSACTION AND CAVEAT FOR CONSUMER USING ATM CARD

A SOHAM BHATT
Student of Master of Business Administration
Chimanbhai Patel Institute of Management and Research,
Gujarat Technological University, Ahmedabad

SWATI SAXENA
Assistant Professor, Chimanbhai Patel Institute of Management and Research
Gujarat Technological University, Ahmedabad

Abstract:

"Total branch automation (TBA) enables customers to transact all their banking needs through a single counter instead of going to different counters in the premises. TBA helps significantly in improving the efficiency of operations." Banking in India is taking a quantum jump after demonetization. Banking sector is matching the pace with digital India movement for transition towards digital economy. The paper examines preparedness and knowledge level of banking consumers towards digital services and caution that needs to be taken. Data has been analysed using SPSS 17.0 And ANOVA has been applied for deriving conclusion. Sample study suggests that Artificial Intelligence & Biometrics are two prominent practices that can curb ATM frauds.

Keywords: *Digital banking products, Financial services, Consumer Caveats, ATM frauds*

INTRODUCTION

"India has a Complex and Integrated Banking and Financial system serving to all the Financial Intermediary requirements of customers. The Banking system is the Most Dynamic Segment of our financial sector, almost 80 % of the funds flow through the financial sector. The macro magnitude of Banking indicates the fact that it is a very big and dynamic sector of the economy. It plays a significant role in the growth of the Indian economy"

An ATM is an electronic device which allows a bank's customer to make cash withdrawals and check their account balance at any time without the need for a human teller.

HOW ATM WORKS

NETWORKING CONCEPT

1. Most ATMs are connected to the authorization of transaction by the card issuer or other authorizing institution via the communication network.

2. Most host computers can support either leased-line or dial-up machines.
3. Leased-line machines connect directly to the host computer through a four-wire, point-to-point dedicated telephone line.
4. Dial-up ATMs connect the host computer through a normal phone line using a modem.
5. The host computer may be owned by a bank or any financial institutions or it may be used by an independent service provider.

DATABASE SECURITY

1. The ATM keeps all the information about the user and user's account inside the centralized database. Inside the database, all the information is stored in the form of tables (objects) which are more secured than the general file systems.
2. The database also provides locking mechanisms to maintain the safety and security of data.

NETWORK SECURITY

The ATM network system provides the following features.

- **Authentication:** The user is the one it claims to be.
- **Confidentiality:** Only authorized users can access the content of the data.
- **Integrity:** The data is not be altered by the third party during the transmission.
- **Non-repudiation (refuse to access):** A user can't deny the fact that it has accessed a service or data.

To Provide Security, Atm System Follows Three Different Mechanism

- **Time out:** - The customer may fail to enter the PIN within the allowed time limit then the card is returned.
- **Invalid card:** - The card is not recognized and it is returned.
- **Stolen card:** - The card is recognized as a stolen card and is retained by the machine.

Table 1 indicates data for ATN related registered complaints from 2015 to 2018.A steady rise in complaints make its inevitable to identify where is the fault in system.

Table 1 Breakup of ATM / Debit Card Complaints

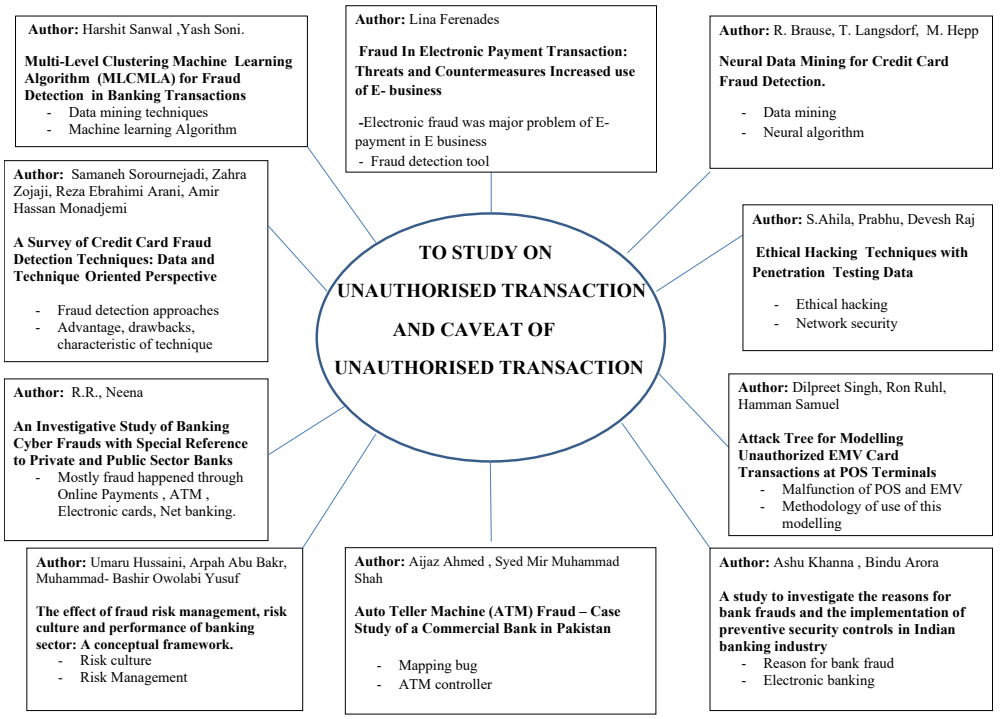
Sub Category	No of Complaints		
	2015-16	2016-17	2017-18
Non-Payment of Cash / Account Debited but Cash not Dispensed by ATMs*	7,095 (6.9%)	9,656 (7.4%)	14,691 (9%)
Short Payment of Cash / *Less or Excess amount of Cash Dispensed by ATMs	1,164 (1.1%)	1,222 (0.9%)	1,166 (0.7%)
*Account Debited More than Once for One Withdrawal in ATMs or for POS Transaction	-	-	965 (0.6%)
	-	-	2,356 (1.4%)

Use of Stolen / Cloned Cards	-	-	2117 (1.3%)
Others	4,822 (4.7%)	5,556 (4.2%)	3,377 (2.1%)
Sub-Total	13,081 (12.7%)	16,434 (12.5%)	24,672 (15.1%)
Total No. of Complaints Received	102,894	130,987	163,590

***Introduced with effect from July 1, 2017 (Figures in bracket indicate % age to total number of complaints of respective years.)**

Source: compiled by author from https://m.rbi.org.in/Scripts/PublicationsView.aspx?id=18948

LITERATURE REVIEW



Source: Created by author

The research paper of Lina Fernandes (March 2013), Several Electronic payments (e-payments) systems have been developed and are increasingly used in e-business. This has given birth to electronic frauds (e-frauds) and it has become a major problem in the electronic payment system. As the internet increases business opportunities, there are new fraudulent and sophisticated techniques being developed by a fraudster.. Several measures for fraud detection and prevention are discussed. this research gives measures to minimize the fraud in e-payment transactions and also the revenue loss

by taking the detective and preventive measures. R. Brause, T. Langsdorf, M. Hepp, consider that the prevention of credit card fraud is an important application for predication techniques. One major obstacle to using neural network training techniques is the high necessary diagnostic quality. This research shows how advanced data mining techniques and neural network algorithm can be combined successfully to obtain a high fraud coverage combined with a low false alarm rate. Recent research (September 2019) for Multi-level clustering machine learning algorithms for fraud detection in banking transactions by Harshit Sanwal and Yash Soni fraud detection methods are continuously developed to defend criminals. In this study, they had focus on the problem of fraud detection in banking transactions. Data mining techniques help in anticipation and detection of fraud. Data mining tools can be used to spot patterns and fraud transactions. Through data mining, factors leading to fraud can be determined. The performance is analysed based on the parameters of the Total Running time and accuracy. Hacking is an activity in which a person exploits the weakness in a system for self-profit or gratification. data and network security is a serious issue that has been studied by Mr. Ahila, Prabhu, Devesh talked about the overview of hacking and how ethical hacking distributes the security.Samaneh Sorournejadi, Zahra Zojaji, Reza Ebrahimi Arani, Amir Hassan Monadjemi in their research paper "A Survey of Credit card fraud detection techniques: data and technique-oriented perspective" credit card becomes an unavoidable part of a household, business, and global activities. This research gives the classification of techniques into two main fraud detection approaches, namely, misuses (supervised) and anomaly detection (unsupervised) is presented.

In the study of Dilpreet Singh, Ron Ruhl and Hamman Samuel, Europay, Mastercard, and Visa (EMV) is a dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. The goal of EMV is to secure debit and credit transaction at a point of sale (POS) terminal, but still, there is a compulsion, which can lead to unauthorized disclosure of cardholder data. the research gave the listing the compulsion leading to various possible attacks EMV payment card transaction process at POs terminal. For the same, they also talked about attack tree methodology that will be used to document these compulsions.

Igntius Majesty Ezeani and Moses okechukwu onyesolu studied. Access codes for building, bank accounts, and computer systems often use personal identification numbers for identification and security clearances. Sometimes PINs and id cards or a password are not altogether reliable. The study of E-Commerce Security Issues and Solutions studied by Niranjanamurthy M, and DR Dharmendra Chahar, E-commerce security is a part of the information security and specifically applied to the components that affect e-commerce that include computer security, data security and other wider realms of the information security framework.

Ashu Khanna and Bindu Arora (2009) studied investigate the reasons

for bank fraud and the implementation of preventive security controls in the Indian banking industry: Their paper identifies the causes responsible for the frauds happening in electronic banking. This paper identifies that the main reason for bank frauds are overburdened staff, lack of training provided, low compliance level, competition. Fernandes,2013.Feuad in electronic payment transaction: threats and countermeasures: this paper gives an overview of electronic payment frauds happing in the present era. It presents clear details about the actual payment frauds and revenue loss due to fraud.

Umaru Hussaini, Arpah Abu Bakr, and Muhammad- Bashir Owolabi Yusuf (2018).talked about the effect of fraud risk management, risk culture, and performance of the banking sector: A conceptual framework. This paper gives a proposed conceptual framework for measuring fraud risk management (preventive, detective and responsive fraud risk management), risk culture and bank performance which could

Concerning the study R.R. & Neena, 2013. An investigative study of banking cyber frauds with special reference to private and public sector banks,throws an emphasis on the series of threats that have been imposed on the safety and accuracy of financial operations due to the increased usage of electronic and digital tools for carrying out business and electronic payment transactions. Frauds mostly happen with online payments, ATMs, electronic cards, and net banking transactions which have been become a serious problem to various banks.

The study examines electronic fraud and credit facilitation of banks in Nigeria(2019). Researchers used secondary data were sourced from central bank Nigeria's electronic fraud forum(NEFF) annual reports for POS, ATM, web, mobile, internet banking.

Aijaz Ahmed and Syed Mir Muhammad Shah talked about Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan(2012). This paper has recommended strong internal controls and fraud screening strategy was also helpfully for the security tool were optimized for their particular product or services

RESEARCH METHODOLOGY

PROBLEM STATEMENT

Unauthorised transaction is taking huge place in the India. Online, debit card/credit card , and ATM transaction fraud are play a major role in this. In the country like India who has huge population there is more need to prevent the unauthorised transaction and increase awareness regarding the same, so this study is conducted to know find the prevention method.

OBJECTIVES OF RESEARCH

- To identify the reasons behind an unauthorized transaction.
- A caveat of an unauthorized transaction for consumers.

RESEARCH DESIGN

- Descriptive

RESEARCH ANALYSIS METHOD

Sample size: 400

Sampling Method: Non Probability Convenience Sampling Method

Sampling unit: ATM cards holders of banks

Statistical Methods : One way ANOVA, Descriptive statistics

Data Analysis tool

- Charts
- SPSS 17.0

ANALYSIS

Hypothesis

1. **H0a:** There is no significant difference between Age and unauthorized transaction and caveat of it's for consumers.

   H1a: There is a significant difference between Age and unauthorized transaction and caveat of it's for consumers.

2. **H0b:** There is no significant difference between Education and unauthorized transaction and caveat of it's for consumer.

   H1b: There is a significant difference between Education and unauthorized transaction and caveat of it's for consumers.

3. **H0c:** There is no significant difference between Profession and unauthorized transaction and caveat of it is for consumer.

   H1c: There is a significant difference between Profession and unauthorized transaction and caveat of it is for consumer.

4. **H0d:** There is no significant difference between Gender and unauthorized transaction and caveat of it is for consumer.

   H1d: There is a significant difference between Gender and unauthorized transaction and Caveat of it is for consumer.

Hypothesis study

1) **H0a:** There is no significant difference between Age and unauthorized transaction and caveat of it is for consumers.

   H1a: There is a significant difference between Age and unauthorized transaction and caveat of it is for consumers.

Table:1 One way Anova analysis of Age Factor

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
Use of ATM	Between Groups	5.321	4	1.330	3.796	.005
	Within Groups	138.439	395	.350		
	Total	143.760	399			
Use of Net banking	Between Groups	7.441	4	1.860	2.285	.060
	Within Groups	321.559	395	.814		
	Total	329.000	399			

Use of Online wallet	Between Groups	15.681	4	3.920	3.877	.004
	Within Groups	399.359	395	1.011		
	Total	415.040	399			
Feeling unsecure while doing ATM transactions.	Between Groups	6.053	4	1.513	1.838	.121
	Within Groups	325.137	395	.823		
	Total	331.190	399			
ATM transaction doing with	Between Groups	5.842	4	1.461	2.948	.020
	Within Groups	195.668	395	.495		
	Total	201.510	399			
Sharing Mobile Number during the online purchase.	Between Groups	4.465	4	1.116	2.129	.077
	Within Groups	207.133	395	.524		
	Total	211.598	399			
Sharing Account Number during the online purchase.	Between Groups	.672	4	.168	.395	.812
	Within Groups	167.806	395	.425		
	Total	168.477	399			
Sharing Cvv during the online purchase.	Between Groups	9.130	4	2.282	6.587	.000
	Within Groups	136.868	395	.347		
	Total	145.997	399			
Sharing Debit/ credit card number during the online purchase.	Between Groups	26.635	4	6.659	9.016	.000
	Within Groups	291.725	395	.739		
	Total	318.360	399			
Sharing IFSC code during the online purchase.	Between Groups	.710	4	.178	.396	.812
	Within Groups	177.287	395	.449		
	Total	177.998	399			
Payment fraud affects consumer confidence in non-cash payments.	Between Groups	15.049	4	3.762	2.641	.033
	Within Groups	562.729	395	1.425		
	Total	577.778	399			
The larger accounts/ transactions are targets of unauthorized transactions than smaller ones.	Between Groups	2.979	4	.745	.562	.691
	Within Groups	523.718	395	1.326		
	Total	526.698	399			
The biometrics system is essential to verify the identity of the user in an ATM.	Between Groups	14.896	4	3.724	3.074	.016
	Within Groups	478.542	395	1.211		
	Total	493.438	399			
There is a need for more security in online transactions.	Between Groups	28.262	4	7.065	5.788	.000
	Within Groups	482.176	395	1.221		
	Total	510.437	399			

Visiting any kind of unknown links, websites, or emails for financial meters.	Between Groups	2.929	4	.732	.631	.641
	Within Groups	458.431	395	1.161		
	Total	461.360	399			
While doing POS transaction does you cover your pin with your hands.	Between Groups	58.352	4	14.588	6.530	.000
	Within Groups	882.488	395	2.234		
	Total	940.840	399			

Interpretation:

According to age factor here, significant value which is less than the 0.05 is rejected null hypothesis and accepted alternative hypothesis. The significant value which is higher than the 0.05 is rejected alternative hypothesis and accepted null hypothesis. So here use of ATM, Use of Online wallet, ATM transaction doing with, sharing CVV and debit/ credit card number during purchasing online, payments fraud affects noncash payments, biometrics systems essential in ATM, need of more security, during POS transaction cover pin. All these parameters have significant difference between age group and rest all factors have no significant difference between age group.

2) H0b: There is no significant difference between Education and unauthorized

transaction and caveat of it's for consumer.

H1b: There is a significant difference between Education and unauthorized transaction and caveat of it's for consumers.

Table:2 One Way Anova Analysis of Education factor

ANOVA						
		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Use of ATM	Between Groups	6.088	3	2.029	5.837	.001
	Within Groups	137.672	396	.348		
	Total	143.760	399			
Use of Net banking	Between Groups	12.566	3	4.189	5.242	.001
	Within Groups	316.434	396	.799		
	Total	329.000	399			
Use of Online wallet	Between Groups	4.750	3	1.583	1.528	.207
	Within Groups	410.290	396	1.036		
	Total	415.040	399			
Feeling unsecure while doing ATM transactions.	Between Groups	.961	3	.320	.384	.765
	Within Groups	330.229	396	.834		
	Total	331.190	399			
ATM transaction doing with	Between Groups	5.359	3	1.786	3.607	.014
	Within Groups	196.151	396	.495		
	Total	201.510	399			

Sharing Mobile Number during the online purchase.	Between Groups	2.866	3	.955	1.813	.144
	Within Groups	208.731	396	.527		
	Total	211.597	399			
Sharing Account Number during the online purchase.	Between Groups	.226	3	.075	.177	.912
	Within Groups	168.251	396	.425		
	Total	168.477	399			
Sharing Cvv during the online purchase.	Between Groups	.681	3	.227	.619	.603
	Within Groups	145.317	396	.367		
	Total	145.998	399			
Sharing Debit/ credit card number during the online purchase.	Between Groups	10.479	3	3.493	4.493	.004
	Within Groups	307.881	396	.777		
	Total	318.360	399			
Sharing IFSC code during the online purchase.	Between Groups	1.043	3	.348	.778	.507
	Within Groups	176.955	396	.447		
	Total	177.997	399			
Payment fraud affects consumer confidence in non-cash payments.	Between Groups	15.251	3	5.084	3.579	.014
	Within Groups	562.526	396	1.421		
	Total	577.777	399			
The larger accounts/ transactions are targets of unauthorized transactions than smaller ones.	Between Grou ps	22.798	3	7.599	5.972	.001
	Within Groups	503.899	396	1.272		
	Total	526.698	399			
The biometrics system is essential to verify the identity of the user in an ATM.	Between Groups	10.863	3	3.621	2.971	.032
	Within Groups	482.575	396	1.219		
	Total	493.438	399			
There is a need for more security in online transactions.	Between Groups	10.441	3	3.480	2.756	.042
	Within Groups	499.997	396	1.263		
	Total	510.437	399			
Visiting any kind of unknown links, websites, or emails for financial meters.	Between Groups	20.328	3	6.776	6.084	.000
	Within Groups	441.032	396	1.114		
	Total	461.360	399			
While doing POS transactions do you cover your pin with your hands.	Between Groups	4.353	3	1.451	.614	.607
	Within Groups	936.487	396	2.365		
	Total	940.840	399			

Interpretation:

According to the education factor here, a significant value which is less than the 0.05 is rejected null hypothesis and accepted alternative hypothesis. The significant value which is higher than the 0.05 is rejected alternative hypothesis and accepted null hypothesis.so here, use of ATM, use of Net banking, ATM transaction doing with, sharing debit/card number during online purchase, payments fraud affects noncash payments, biometrics systems essential in ATM, need of more security, larger accounts more affected unauthorized transaction, visiting any kind of unknown links, websites or emails for financial meter All these parameters have significant difference between education and rest all factors have no significant difference between education group.

3) H0c: There is no significant difference between Profession and unauthorized transaction and caveat of it's for consumer.

H1c: There is a significant difference between Profession and unauthorized transaction and caveat of it's for consumer

Table:3 One Way Anova Analysis of Profession factor

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
Use of ATM	Between Groups	6.847	4	1.712	4.938	.001
	Within Groups	136.913	395	.347		
	Total	143.760	399			
Use of Net banking	Between Groups	33.068	4	8.267	11.034	.000
	Within Groups	295.932	395	.749		
	Total	329.000	399			
Use of Online wallet	Between Groups	23.835	4	5.959	6.017	.000
	Within Groups	391.205	395	.990		
	Total	415.040	399			
Feeling unsecure while doing ATM transactions.	Between Groups	10.983	4	2.746	3.387	.010
	Within Groups	320.207	395	.811		
	Total	331.190	399			
ATM transaction doing with	Between Groups	5.430	4	1.357	2.734	.029
	Within Groups	196.080	395	.496		
	Total	201.510	399			
Sharing Mobile Number during the online purchase.	Between Groups	2.141	4	.535	1.010	.402
	Within Groups	209.456	395	.530		
	Total	211.598	399			
Sharing Account Number during the online purchase.	Between Groups	3.484	4	.871	2.085	.082
	Within Groups	164.993	395	.418		
	Total	168.478	399			
Sharing Cvv during the online purchase.	Between Groups	3.854	4	.964	2.678	.032
	Within Groups	142.143	395	.360		
	Total	145.998	399			
Sharing Debit/ credit card number during the online purchase.	Between Groups	10.281	4	2.570	3.295	.011
	Within Groups	308.079	395	.780		
	Total	318.360	399			

Sharing IFSC code during the online purchase.	Between Groups	2.270	4	.568	1.276	.279
	Within Groups	175.727	395	.445		
	Total	177.998	399			
Payment fraud affects consumer confidence in non-cash payments.	Between Groups	8.776	4	2.194	1.523	.195
	Within Groups	569.001	395	1.441		
	Total	577.777	399			
The larger accounts/ transactions are targets of unauthorized transactions than smaller ones.	Between Groups	5.769	4	1.442	1.094	.359
	Within Groups	520.928	395	1.319		
	Total	526.698	399			
The biometrics system is essential to verify the identity of the user in an ATM.	Between Groups	10.908	4	2.727	2.232	.065
	Within Groups	482.530	395	1.222		
	Total	493.438	399			
There is a need for more security in online transactions.	Between Groups	31.294	4	7.824	6.450	.000
	Within Groups	479.143	395	1.213		
	Total	510.438	399			
Visiting any kind of unknown links, websites, or emails for financial meters.	Between Groups	5.586	4	1.397	1.210	.306
	Within Groups	455.774	395	1.154		
	Total	461.360	399			
While doing POS transactions do you cover your pin with your hands.	Between Groups	21.907	4	5.477	2.354	.053
	Within Groups	918.933	395	2.326		
	Total	940.840	399			

Interpretation

According to the Profession factor here, a significant value which is less than the 0.05 is rejected null hypothesis and accepted alternative hypothesis. The significant value which is higher than the 0.05 is rejected alternative hypothesis and accepted null hypothesis.so here, use of ATM, use of net banking, use of the online wallet, feeling unsecured while doing a transaction, ATM transaction doing with, sharing CVV and debit/card number during online purchase, need of more security in an online transaction. All these parameters have significant difference between professions and rest all factors have no significant difference between professions.

4) H0d: There is no significant difference between Gender and unauthorized transaction and caveat of it's for consumer.

H1d: There is a significant difference between Gender and unauthorized transaction and caveat of it's for consumer.

Table:4 One Way Anova Analysis of Gender factor

ANOVA		Sum of Squares	df	Mean Square	F	Sig.
Use of ATM	Between Groups	6.600	2	3.300	9.551	.000
	Within Groups	137.160	397	.345		
	Total	143.760	399			
Use of Net banking	Between Groups	16.302	2	8.151	10.348	.000
	Within Groups	312.698	397	.788		
	Total	329.000	399			
Use of Online wallet	Between Groups	12.084	2	6.042	5.953	.003
	Within Groups	402.956	397	1.015		
	Total	415.040	399			
feeling unsecure while doing ATM transactions.	Between Groups	1.730	2	.865	1.043	.354
	Within Groups	329.460	397	.830		
	Total	331.190	399			
ATM transaction doing with	Between Groups	3.700	2	1.850	3.713	.025
	Within Groups	197.810	397	.498		
	Total	201.510	399			
Sharing Mobile Number during the online purchase.	Between Groups	2.129	2	1.064	2.018	.134
	Within Groups	209.469	397	.528		
	Total	211.597	399			
Sharing Account Number during the online purchase.	Between Groups	.969	2	.485	1.149	.318
	Within Groups	167.508	397	.422		
	Total	168.477	399			
Sharing Cvv during the online purchase.	Between Groups	.531	2	.265	.724	.485
	Within Groups	145.467	397	.366		
	Total	145.998	399			
Sharing Debit/ credit card number during the online purchase.	Between Groups	3.449	2	1.725	2.174	.115
	Within Groups	314.911	397	.793		
	Total	318.360	399			
Sharing IFSC code]during the online purchase. [	Between Groups	2.563	2	1.281	2.900	.056
	Within Groups	175.435	397	.442		
	Total	177.997	399			
Payment fraud affects consumer confidence in non-cash payments.	Between Groups	4.100	2	2.050	1.419	.243
	Within Groups	573.678	397	1.445		
	Total	577.778	399			
The larger accounts/ transactions are targets of unauthorized transactions than smaller ones.	Between Groups	2.677	2	1.338	1.014	.364
	Within Groups	524.021	397	1.320		
	Total	526.698	399			

The biometrics system is essential to verify the identity of the user in an ATM.	Between Groups	1.629	2	.815	.658	.519
	Within Groups	491.808	397	1.239		
	Total	493.437	399			
There is a need for more security in online transactions.	Between Groups	2.929	2	1.464	1.146	.319
	Within Groups	507.509	397	1.278		
	Total	510.437	399			
Visiting any kind of unknown links, websites, or emails for financial meters.	Between Groups	4.173	2	2.087	1.812	.165
	Within Groups	457.187	397	1.152		
	Total	461.360	399			
While doing POS transactions do you cover your pin with your hands.	Between Groups	1.950	2	.975	.412	.662
	Within Groups	938.890	397	2.365		
	Total	940.840	399			

Interpretation

According to the Gender factor here, a value which is less than the 0.05 is rejected null hypothesis and accepted alternative hypothesis. The significant value which is higher than the 0.05 is rejected alternative hypothesis and accepted null hypothesis.so here, use of ATM, use of net banking, use of the online wallet, ATM transaction doing with. Only these parameters have significant difference between gender and rest all factors have no significant difference between gender.

5. Findings

According to research some parameters impact on factors and some were not so that parameters according to factors as below,

Particular	Impacted Parameters	Non impacted parameters
Age Factor	• Use of ATM • Use of Online wallet • ATM transaction doing with, • Sharing Cvv and debit/cards number during purchasing online • Payment fraud affects noncash payments. • Biometrics systems essential in ATM • Need for more security in an online transaction. • During POS transaction cover PIN	• Use of Net Banking • Feeling unsecured while doing the transaction in ATM • Sharing mobile number and IFSC code during an online purchase • The large accounts/transaction targets of the unauthorized transaction • Visiting any kind of unknown links, email or website

Education Factor	• Use of ATM • Use of Net banking • ATM transaction doing with • sharing debit/card number during an online purchase • payments fraud affects noncash payments • biometrics systems essential in ATM • The need for more security, • Larger accounts more affected unauthorized transaction, • Visiting any kind of unknown links, websites or emails for financial meter	• Use of Online wallet • Feeling unsecured while doing the transaction in ATM • Sharing mobile number, account number, CVV and IFSC code during an online purchase • During POS transaction cover PIN
Profession Factor	• Use of ATM • Use of net banking • Use of online wallet • Feeling unsecured while doing transaction • ATM transaction doing with • Sharing CVV and debit/card number during online purchase, • Need for more security in an online transaction	• Sharing mobile number, account number, and IFSC code during an online purchase • payments fraud affects noncash payments • biometrics systems essential in ATM • The large accounts/transaction targets of the unauthorized transaction • During POS transaction cover PIN.
Gender Factor	• Use of ATM • Use of net banking • Use of online wallet. • ATM transaction doing with	• Feeling unsecured while doing transaction • ATM transaction doing with • Sharing CVV and debit/card number during online purchase, • Need for more security in an online transaction. • Sharing mobile number, account number, and IFSC code during the online purchase • payments fraud affects noncash payments • biometrics systems essential in ATM • The large accounts/transaction targets of the unauthorized transaction • During POS transaction cover PIN

Based on the above table researcher can find that the impacted parameters have significant differences respected to a particular factor and non-impacted parameters have not significant difference so, non-impacted parameters behave the same as per their factor.

Suggestions

- Install a biometric system in ATM for the identity of a customer. (is it costly but easy to install because banks have fingerprints of all the customers in their Aadhar Cards)
- Develop AI so that while wearing a face mask, cap, or handkerchief

on face no one can do transactions in ATM. It will reduce the unauthorized transaction.

- Banks have to increase awareness camping regarding unauthorized transactions through direct dealing with customers.
- For online transactions or net banking, banks can develop 3 step verification now banks have 2 step verification which is id-password and OTP. But they should develop a 3rd step which is the standard question. It works like when customer open net banking or online banking account at that time banks or system gives them option to choose the standard question and its answer should be in word, alphabet(excluding name), or symbol not a numeric. After that when the customer will do the transaction after the OTP this question will be displayed and the customer has to input that answer for that system will give them 3 or 4 seconds. So through this hacking and online transaction fraud and account takeover will be reduced.
- There should be rules for customers that they can operate his/her online account from another phone or computer or laptop within 2 or 3 times a month.

Conclusion

Through the present research, it has been concluded The majority of the customers do not follow the guidelines of the RBI and the majority of the customers aren't aware of the RBI's guidelines regarding Unauthorized transactions. Need for standard procedures to prevent unauthorized transactions and need of good machinery because some of the customers are not using the ATMs due to the malfunctioning of the machine. Some of the customers are not using online wallets or net banking due to errors and sometimes they are facing issues like amount was debited but not credit in another account.

REFERENCES

Aijaz Ahmed Shaikh, S. M. (October 2012). Auto Teller Machine (ATM) Fraud – Case Study of a Commercial. ***International Journal of Business and Management;*** Vol. 7, No. 22.

Ashu Khanna, B. A. (2009). A study to investigate the reasons for bank fraud and the implementation of preventive security controls in the Indian banking industry. Int. ***Journal of Business Science and Applied Management,*** Volume 4, Issue 3.

Dilpreet Singh, R. R. (2017). Attack Tree for Modelling Unauthorized EMV Card Transactions at.

Fernandes, L. (March (2013)). Fraud In Electronic Payment Transactions: Threats and Countermeasures. ***Asia Pacific Journal of Marketing & Management Review.***

Harshit Sanwal, Y. S. (September-2019). Multi-Level Clustering Machine Learning Algorithm (MLCMLA) for Fraud Detection in Banking Transactions. ***International Journal of Engineering Research & Technology (IJERT).***

Hepp, R. B. (n.d.). Neural Data Mining for Credit Card Fraud Detection. Gesellschaft f. Zahlungssysteme GZS, Frankfurt a. M., Germany.

Kelechukwu Stanley (Ph.D.), C. (. (October 2019). Electronic Fraud and Credit Facilitation of Banks In Nigeria. ***Journal of Accounting Information and Innovation.***

Moses Okechukwu Onyesolu, I. M. (April 2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. ***International Journal of Advanced Computer Science and Application.***

Niranjanamurthy M, D. D. (July 2013). The study of E-Commerce Security Issues and Solutions. ***International Journal of Advanced Research in Computer and Communication Engineering.***

S. Ahila, A. D. (2019). Ethical Hacking Techniques with Penetration Testing. ***International Journal of Engineering Research & Technology (IJERT).***

SamanehSorournejad, Z. Z. (n.d.). A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective.

Soni R.R., S. N. (July,2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks. ***Research Journal of Management Sciences*** ISSN 2319–1171.

Umaru Hussaini, A. A.-B. (January,2019). The effect of fraud risk management, risk culture, and performance of the banking sector: A conceptual framework. ***International Journal of Multidisciplinary Research and Development.***