NOLEGEIN Journal of
Management Information Systems

ISSN: 2581-6810
Volume 4, Issue 2, 2021
DOI (Journal): 10.37591/NJMIS

http://mbajournals.in/index.php/JoMIS/index

Research NJMIS

A Case Study on Analysis of Fraud Issues in E-tailing

V.R. Hiremath[1,]*, Sanjeev Ingalagi[2]

Abstract

India has gone through a huge transformation shifting its gear from traditional to modern methods of retailing in 21st century and developed countries have already implemented and channelized the profit out it. The society of developed countries has also acknowledged this revolution. The globalization has led to transformation in technology and e-tailing for business and consumer related services. In recent years, e-tailing has acquired a prominence in market but also had alarming increase in fraud issues in online shopping. But India is still far from this transformation and it is in adequacy to implement a proper law. The study focuses on the different fraud issues of e-retailing and how this has impacted the society by creating hurdle in accepting e-retailing in a developing country like India. My research identifies the answers required to create the changes in modern e-retailing. The research also provides a deep insight to the business into implement the solution in business edifices by understanding the demands of the future market. The emergent countries have taken concrete decisions to understand the future needs of customers and serve them in a globalized world.

Keywords: Globalization, business, retailing, information technology, e-tailing

INTRODUCTION

The Indian market has witnessed a revolution in e-retail market. The digitalization has cemented multifaceted ways to the consumer to make his life more comfortable than ever. Today, all the online buying happens only on the fingertips of individuals by ordering food, book travel tickets, electronic goods etc. The consumer making decisions through finger tips does not know that he is obliged to himself to the set of norms and conditions without assessing the future consequences of it. Online fraud is way of deceiving the other party with the intention to harm the individual [1]. The study analyses the current issues of online fraud and comprehensive review of the issues and prevention of online fraud. The study also testifies the e-fraud with the changing circumstances in the light of online shopping. The study also addresses the problems faced by the e-consumer and understand that where does the Indian law stands and how it is operational to respond to the issues of e-consumers in online frauds [2].

***Author for Correspondence**
V.R. Hiremath
E-mail: viruhiremath10@gmail.com

[1]Research Scholar, Department of Management, Gogte Institute of Technology, Belagavi, Karnataka, India
[2]Associate Professor, Department of Management, Gogte Institute of Technology, Belagavi, Karnataka, India

Received Date: October 26, 2021
Accepted Date: November 10, 2021
Published Date: December 12, 2021

Citation: V.R. Hiremath, Sanjeev Ingalagi. A Case Study on Analysis of Fraud Issues in E-tailing. NOLEGEIN Journal of Management Information Systems. 2021; 4(2): 18–27p.

AIMS

1. To study the fraud issues involved in e-tailing.
2. To understand the formation of e-fraud issues.
3. To examine the e-fraud issues.
4. To identify new ways to resolve the e-fraud issues in future.

METHODS

Coverage of the Study

This research work is restricted to study of online deception of e-tailing in India.

Source of Data

The study is based on secondary information and is limited B2C online shopping.

Data Analysis

Analysis of data and information collected from published sources were made keeping the objectives of the study in mind [3].

ANALYSIS OF E-FRAUD ISSUES

Courtesy: Federal Trade Commission Report

The world is moving towards transformation of technology and one of the dark side is misuse of technology which is depicted in below diagram. In recent years, there is very severe surge in the online frauds due to various reasons like technology inefficiency, ineffective law implementation, and online trends which are changing at a very fast pace [4, 5].

The fast moving online business also opens window to the fraudster to increase the unethical schemes against business establishment. The websites and Apps are getting more traffic generated for business all over the countries. It is found that the deceptive digital operation attempts against business originating from India have enlarged 28.32% compared to the previous year [6]. The suspected highest digital fraudulent transactions have happened in three major cities like Mumbai, Chennai and Delhi (Figure 1).

Courtesy: Fraud and Abuse Report, Arkose Labs Global Network, Courtesy: Federal Trade Commission Report

In 2020, there was surge and change in the geographies where the fraud attacks initiated. The majority of attacks are originated from the countries with developing economies, where employment opportunities are limited and low poverty. Typically this situation becomes fertile grounds for the fraudster to do their illegal activities (Figure 2).

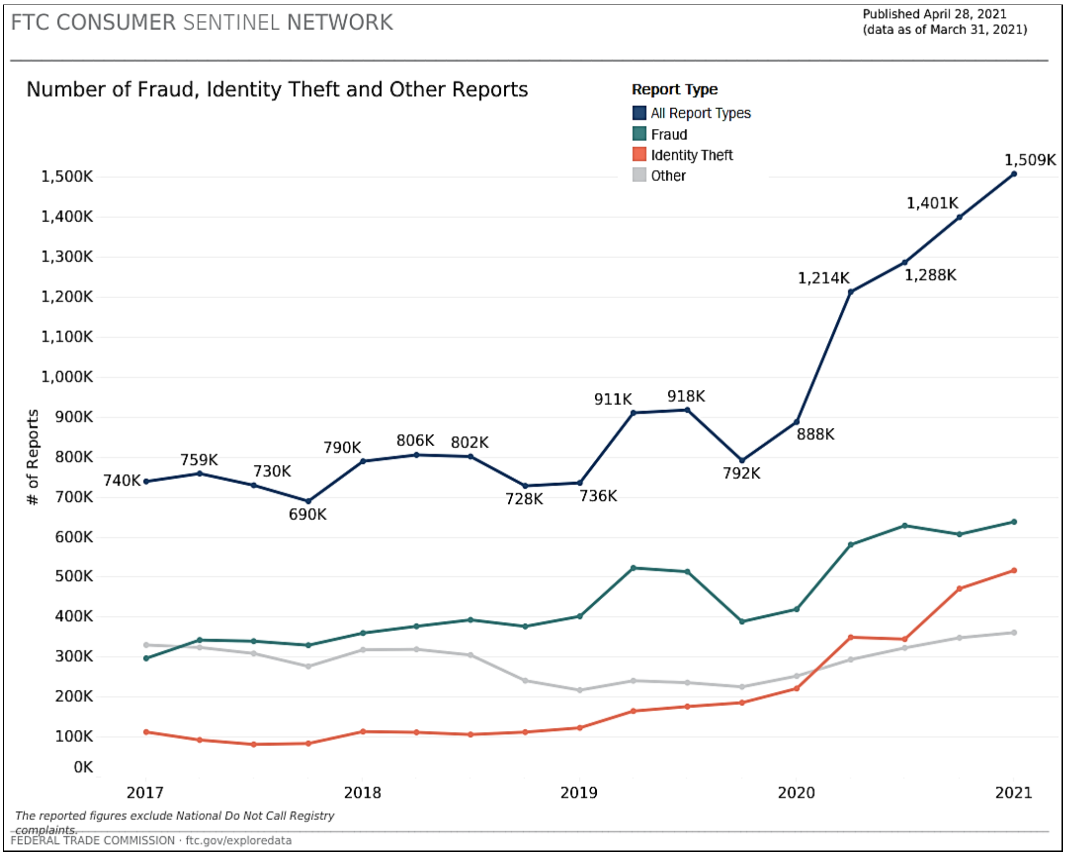

Figure 1. 2021 Federal Trade Commission Report.

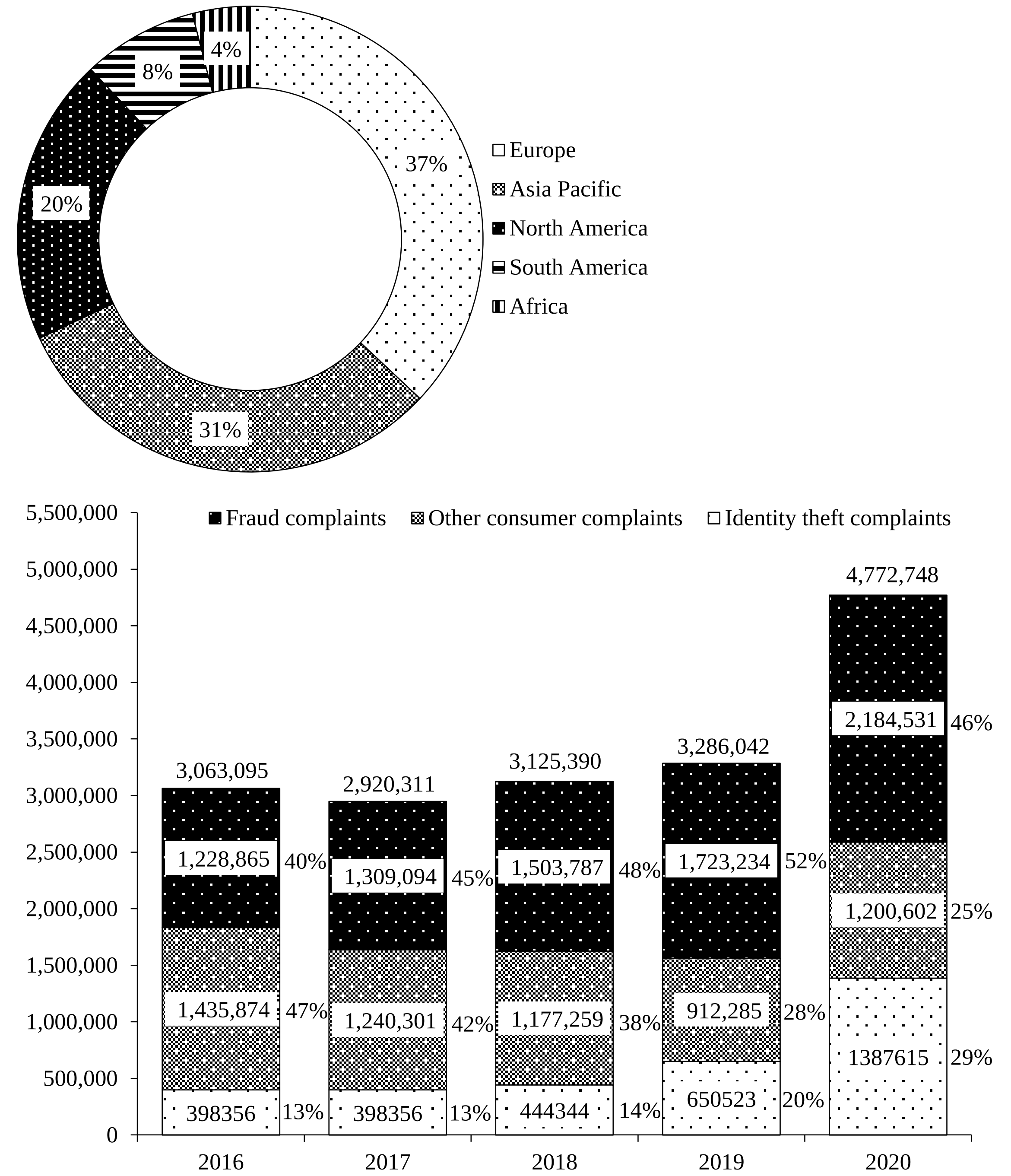

Figure 2. Fraud Attacks in different Continents.

Europe stands at top in overall fraud attacks, followed by Asia which is traditionally active fraud hub. The United States, especially North America, had a spike in fraud attacks. A great number of attacks have originated from Russia with some spike in malicious activity from major economies in Western Europe. As per federal trade Commission report in 2020, which shows that there is increase in the frauds compared to the previous year [7]. The lunacy of laws will give the opportunity to the fraudsters to look for the new ways and take advantage of inefficiencies of norms and benefit the same in an unethical gain. If the present situation is not handled in a proper way, it would create havoc in fraud attacks and create distrust among customers and the online shopping business in the world. There is alarming situation to curb the crime from its root, otherwise it will have severe effects on the individual privacy, trust and security issues [8, 9].

Courtesy: Federal Trade Commission Report

The econsumer.gov International Fraud Report shows that the consumers have been victimized of fraud cases. In quarter of 2021, the international e-consumer has got 13,127 reports with $59.57 million losses with 87% reported of loss due fraud in the world. The top consumer location from where the fraud activities happened are from United States of America with 4,638 cases and India Stands at 4th position with 376 cases. The above report is only based on the complaint received from e-consumer.gov but there may be many more cases which are not unfolded due to not complaining and unawareness of the fact of the international agencies [10]. In India, vulnerability to such crime is high

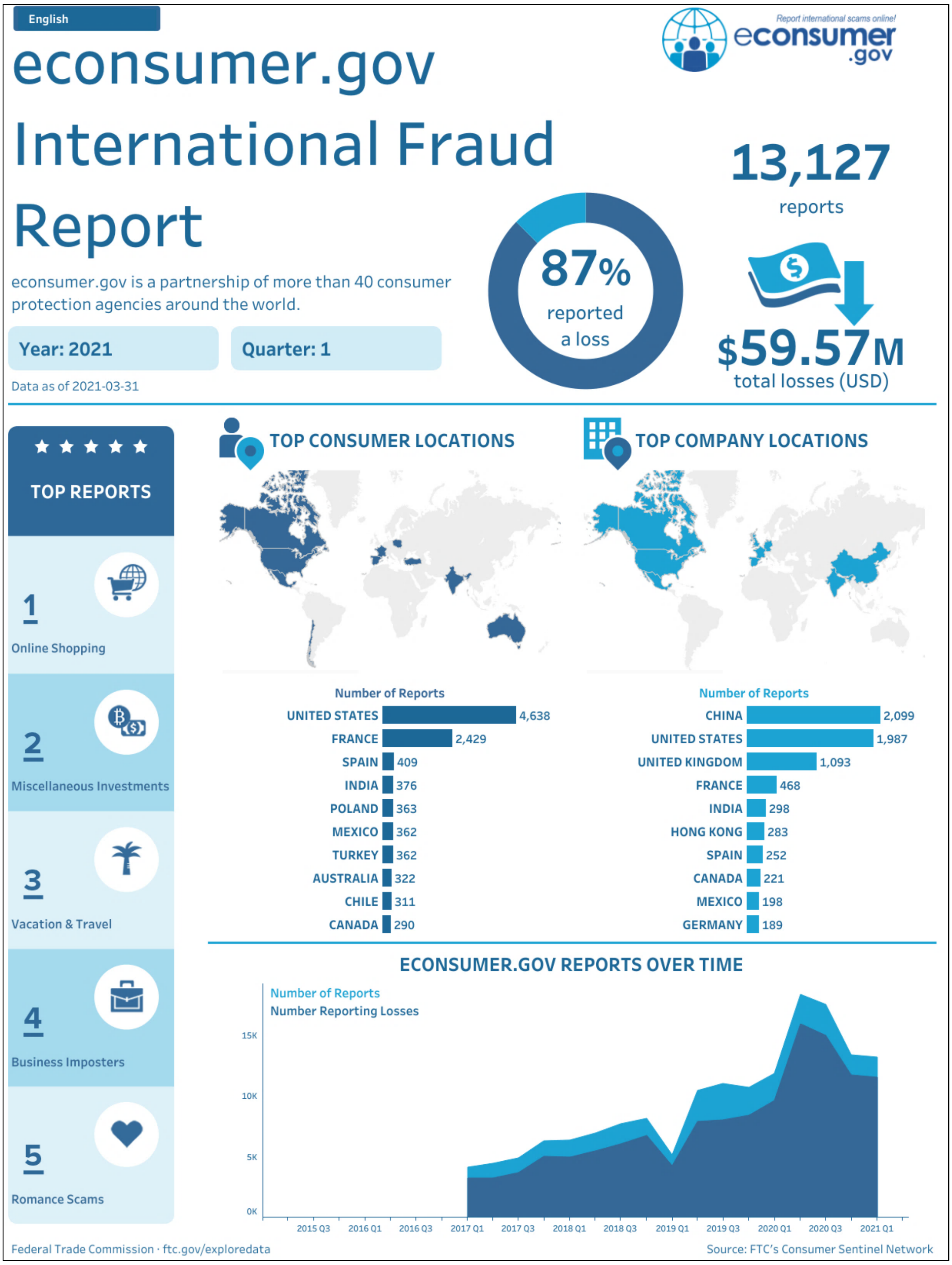

Figure 3. International Fraud Report 2021 Q1.

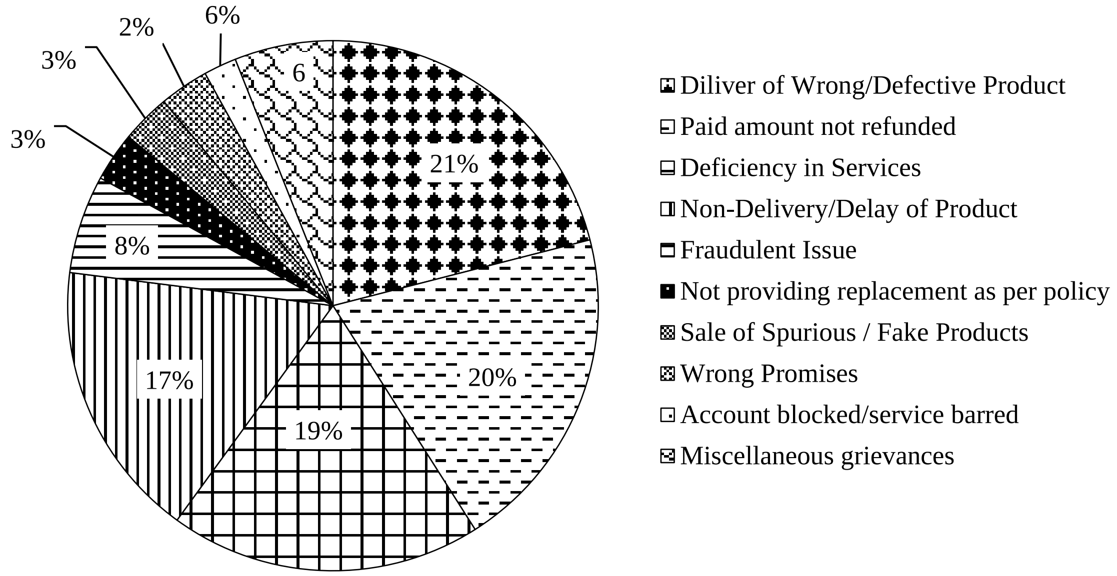

Figure 4. Categories of fraud in Online Shopping.

due to illiterate consumer, unaware of rights, and Government's failure to implement and create awareness about these crimes. The top locations where the company have been located to drive these frauds are more in China with 2099 reports, and India at 5th position with 298 reports, which clearly indicates that there are more number of unauthorized companies which are due in operation under the umbrella of government and its ineffective laws [11]. The report shows that the online shopping stands at 1st place where it becomes easy for the intruder to access other credentials and commit crime (Figure 3).

The online shopping is becoming a platform for cybercriminals to target the customers. The digital world will give enormous prospect for the criminals to access the millions of personal credentials which are easily available on the dark web. This gives opportunity for fraudsters to hide their true identity and operate on false identity without the permission of true owner of credentials [12].

The most common type of fraud is of delivery of wrong product or defective product which amounts to 21%. The defective product delivery or wrong delivery happens intentionally at the intermediaries where they exchange the product or misplace the product before it is delivered. In a very rare case, company will send a defective product [13]. The paid amount not refunded is of 20% which speaks that while buying the product, the process is made for transaction of the money but when you want to reject the goods for certain reasons and get refund of the amount, the company humiliates and takes at least of 1 to 3 months and most of the times the amount is not refunded (Figure 4).

The main aim of the online shopping companies is to give a standard delivery in the products which they sell through online business. But most of standards which they state in their website are not practically implemented because of which we come across deficiency in services, delay of product, not providing replacement, selling fake products and making false promises [14]. The Global online shopping companies are struggling to resolve a fake new account creation. The cyber criminals would employ more bots to create fake accounts at a large scale, which would be used to commit wide range of frauds in the world. The homegrown laws, solutions and different norms are ineffective at stopping these attacks and also hinder the customer experience [15].

CONCLUSION

Due to feasibility in acceptance of technology and viability of internet, there is potential increase in the e-commerce market in India. The changing work habits and consumers opting for adaptability and convenience had made the consumers to adopt the new ways of buying the products with minimum diligence. The online fraud cannot be addressed in terms of the mechanical changes but need to change the fundamentals of relationship and subject matter and expectations of consumers according to the changing situation and issues of time. India has responded to technological changes and enacted Information technology act 2000, Companies Act 2013, Consumer Protection act 2019 according to the changing conditions to curtail the culprits. The true justice lies when government responds to the true spirits of law and justice to uncover the fraud and save the consumer from being exploited.

RECOMMENDATIONS

Online fraud is criminal deception conducted during a commercial transaction over the internet with the goal of financial or personal gain of the fraudsters while negatively affecting the bottom line of the merchant.

1. There is inconsistent or mismatch between IP address and the email address or mismatch.
2. There are red flags with multiple units having same SKU within one order.
3. If your purchases are from unusual location which is uncommon and which you do not use that IP address (For e.g., Uganda).
4. If the buyer is having multiple purchases in one order but product delivery is having different address.
5. Always the fraudster will do multiple purchases with back to back orders.
6. Fraudster has multiple orders with credit orders over longer period.
7. Fraudster has multiple declined transactions in a row with more than 10 attempts.

IMPLEMENTATIONS

1. The customer should always check the small padlock of the website whether it starts with “http”-Danger or “https”–Safe. https means the website is secured.
2. Buyer is buying from an unknown e-commerce company or if you are buying for first time, then use cash on delivery method.
3. Consumer should always read the terms and conditions and confidential policies of the e-commerce company.
4. Consumer should provide all the contact details with clear mail ID, mobile number and postal address.
5. Consumer should know the warranty terms, and usage of product before you decide to buy.
6. Consumer should make sure for encryption key in the payment gateway to understand that the payment made by the consumer is safe.

REFERENCES

1. IBEF (Indian Brand Equity Foundation) Report on e-commerce. 2018.
2. Law & Technology: Evolving challenges as a result of fraud in E-commerce Sector. ASSCHOM Report.
3. http://www.mruni.eu/lt/mokslo_darbai/jurisprudence
4. Economic Times News Paper. 2017 May 10, 8.27 IST, ET Retail.com.
5. IAMAI and IMRB International Report on E-commerce.
6. Zeithaml VA. Service excellent in electronic channels. Manag Serv Qual. 2002; XII(3): 135–138.
7. http://www.thehindubusinessline.com/features/smartbuy/tech-news/amazons
8. Susheel Barath K, Mahalakshmi V. Legal Issues in E-Commerce Transactions-an Indian Perspective. Int J Recent Innov Trends Comput Commun. 2016 Nov; 4(11): 184–191.
9. International Fraud Report. econsumer.gov.
10. Annual Consumer Report 2019-2020. Department of Consumer Affairs, Ministry of Consumer Affairs, Food & Public Distribution, Government of India; 2020.
11. Nishith Desai Associates. (2015 Jul). E-Commerce in India. Legal, Tax and Regulatory Analysis. [Online]. www.nishithdesai.com.
12. National Report on E-commerce Development on India. Inclusive and Sustainable Industrial Development Working Paper Series WP 15. Submitted to UNIDO (United Nation Industrial Development organization); 2017.

13. IANS. (2021 Apr 29). New Study Shows Spike in Digital Fraud Attempts from India. [Online]. https://www.nationalheraldindia.com/india/new-study-shows-spike-in-digital-fraud-attempts-from-india
14. http://consumeraffairs.nic.in/consumer/writereaddata/e-Retailingindia.pdf. Priyanka Joshi, Hemant Upadhyay.
15. http://consumeraffairs.nic.in/consumer/writereaddata/e-Retailingindia.pdf

APPENDIX

Target Group

1. The Tech-savvy consumers.

Learning Objectives

1. The objective of this case understands the fraud issues in online shopping and how the present operational law of India is responding to it.

Key Issues

1. Friction between law and society.
2. Fraud issues are spiking.
3. Operational law failing to address the issue.
4. How future frauds can be prevented?

Questions for Discussion

1. What are the ways in which frauds in online shopping are happening today?
2. The present law gives scope for online shopping fraud or the operational law is not implemented properly.
3. What is the future course of action to prevent fraud in online shopping?

Possible Answers to the Questions

1) Types of Online Shopping Frauds

i) Identity Theft

Identity theft is a type of crime where the fraudster persons present identifiable information without the consent of the person who is having real identity. The fraud effects the customer and the company and questions the safety of the information which the customer has put at the time of transaction.

ii) Chargeback Fraud

This is also known as friendly fraud. In this type of fraud, the customer keeps the goods/products purchased online from the e-commerce shop but still asks for a refund stating purchase never made or payment being made twice or item was never received. Having a clear refund, reshipping, tracked shipping, and return policies for the e-store may help to reduce this ‘friendly’ fraud.

iii) Clean Fraud

This fraud is done with the stolen credit card from a genuine user and is used to make an online purchase. The stolen card and card holder’s information is used to commit the fraud which looks like a legitimate purchase made by verified customers.

iv) Phishing

In phishing personal information of a genuine user like user id, card number, password, and other credit card information is collected via a fraudulent SMS or an email and used to make an online purchase illegally or without the owner’s knowledge. In this type, the user generally gets an SMS or email requesting personal data or a false link to install the malware to obtain this personal data. The fraudster often pretends to be a trusted company or source to ask such information.

v) Triangulation Fraud

In this type of fraud, the fraudster creates a fake online shop offering goods/products at cheap prices. These web shops are used to collect credit card data from the customers who visit the site. When the order is placed, the fraudster orders the product from the real website/merchant using the stolen credit card information and sends that product to the customer. Fraudster gains the payment for the goods and the customer ends up paying twice: once for the fraud store and once for the actual price to the real merchant.

2) India has a robust judiciary and is playing an important role in providing justice. Despite of having so many good laws, there are still so many crimes happening in our country. The country has adequate laws but the main issue arises in its implementation. Poor implementation of laws often leads to inefficiencies and crimes in the society.

i) Some Examples of Poor Law Implementation in India

1. The environmental laws like environment protect and forest conservation act are not implemented correctly and there is no special court to deal with it.
2. The gender equality in India is not correct and there is lot of discrimination in India.
3. Child labour laws are not implemented at the ground level.
4. The right to information act 2005 has been implemented poorly and is having poor quality orders.

ii) Reasons for the Poor Implementation of Laws in India

1. In India, the cases are more but conviction rate is low.
2. The state governments are not implementing the laws appropriately due corruption and lack of funds.
3. There is always rift between state and central government.
4. In India, political will is lacking because politicians make false promises at the time of elections.
5. The norms are normally not implemented in a proper way.
6. The high population makes it difficult to implement the laws.
7. Corruption is one of the base roots of all problems in India and it is difficult to correct it.
8. The people in India are having a habit of breaking the laws despite being educated in laws and norms.

iii) Solution to Improve Law Implementation

1. Proper allocation of the resources to all areas and proper implementation of the active laws to improve the punishment rates.
2. The post review of laws for understanding the law is correct or wrong.
3. The central and state laws should be consistent with each other.
4. The citizens should be aware of the present laws and its punishment for breaking the rules.

3) Future Fraud Prevention in Online Shopping

i) Conduct Site Security Audits on a Regular Basis

- Is the software and plugins for our shopping cart up to date?
- Is our SSL certificate up to date and operational?
- Is our business PCI-DSS (Payment Card Industry Data Security Standard) compliant?
- Do we regularly back up our internet store?
- For admin accounts, hosting dashboards, CMS, database, and FTP access, are we using strong passwords?
- Do we scan our website for viruses on a regular basis?
- Is communication between our store and our consumers and suppliers encrypted?
- Have we deleted any plugins that are no longer in use?

ii) Ensure That Your Store Complies with PCI Standards

If you run an online store that accepts credit card payments, PCI compliance is necessary. PCI compliance is required if you run an online store that takes credit card payments. PCI is the abbreviation for Payment Card Industry. The PCI Security Standards Council develops and manages PCI compliance standards to protect the security of credit card transactions in the payments sector. PCI compliance refers to the fact that your online store and company processes adhere to the PCI requirements. If you run an e-commerce store using a SAS platform, your platform will usually provide this compliance.

iii) Keep an Eye on Your Site for Strange Activities on a Frequent Basis

Shoplifters are caught by fraud prevention officers hired by brick-and-mortar establishments. You can safeguard your online store from fraudulent transactions by keeping an eye on it for unusual behaviour. Keep an eye on your accounts and transactions for red flags including inconsistencies in billing and shipping information, as well as your customers' physical whereabouts. Use technologies that track client IP addresses and alert you to any addresses from nations that are known to be a fraudster's hotspot.

iv) Make use of a Service that Verifies Addresses (AVS)

Address Verification Services are typically offered by credit card processors and issuing banks to detect suspect credit card transactions in real time and prevent credit card fraud. The Address Verification Service compares the card user's (customer's) billing address to the cardholder's billing address on file with the issuing bank. This check is performed as part of the merchant's request to the payment processor for credit card transaction authorization. When the addresses do not match, the system either rejects or flags the transaction for further inquiry.

v) All Purchases Should Require Card Verification Value (CVV) Numbers

The Card Verification Value (CVV) or Card Security Number is the three-digit security code on the back of VISA®, MasterCard®, and Discover® credit and debit cards, and the four-digit security code on the back of American Express® credit and debit cards (CSC). You may confirm that customers have the physical credit card in their possession by requiring all buyers to provide this code for every transaction. This keeps you protected and helps to avoid fraud.

vi) Make use of HTTPS (Secure Hypertext Transfer Protocol) (HTTPS)

HTTPS is a secure version of HTTP, which is the most used protocol for sending data between a customer's web browser (such as Google) and your online store. To protect sensitive information including client names, addresses, and credit card numbers, HTTPS encrypts the data. Using HTTPS protects your online store's transactions from being broadcast in a way that hackers, cybercriminals, and fraudsters can easily see. By purchasing an SSL certificate, you can use HTTPS.

vii) Don't acquire too Much Personal Information from Your Customers

Collecting and storing as little client data as possible is one strategy to secure your store in the event of a data breach or hack. Hackers cannot take your data if you do not have it. As a result, just collect the information required to complete a transaction and ship the merchandise. Collecting Social Security numbers, birth dates, and other sensitive consumer information is not necessary.

viii) Set spending Limitations

Set restrictions for the number of purchases and total cash value you will accept from one account in a single day based on your order and revenue trends. This keeps your exposure to a bare minimum in the event of fraud.

ix) Verify That the IP Address and Credit Card Address are Identical

Every order placed on your website originates from a public IP address (a string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over the Internet). The city or region of the world where the purchaser is making the transaction can generally be deduced from the IP address. This is a red flag if the city or region does not match the address on the credit card being used.

Theories for Discussion

Use of the Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is an information system theory. It focuses on computer users as models, demonstrating how individuals can accept and adopt new technologies. It was created with the goal of predicting user technology adoption decisions. To predict, the Technology Acceptance Model is commonly employed. It means that there are only two factors that influence whether or not a computer system is accepted by its users. The perceived usefulness and simplicity of use of the system are the two factors that influence computer acceptability. The fundamental goal of this strategy is to emphasise the consumers' potential. In other words, it emphasises, for example, when a technology's developer believes that his or her system is user-friendly. Users, on the other hand, will not adopt the system until the creators communicate the technology's benefits and advantages.

The degree to which a computer system user believes that adopting a particular computer system will improve his or her performance, is the perceived usefulness component of the Technology Acceptance Model. It usually relates to a customer's perceptions depending on their experience's outcome. Many businesses, particularly in the banking industry, have acknowledged the presence of perceived utility. In other cases, it is viewed as a determinant of real behaviour in which a user is encouraged to employ an innovative and user-friendly self-service technology to improve and build greater autonomy in conducting certain banking tasks such as transactions. The perceived usefulness component, on the other hand, is rooted in the banking business. It is dependent on the bank's services, such as loan applications, checking balances, and paying utility bills. For example, it is a crucial component in this industry since it influences how well innovation adapts.

The perceived simplicity of use of the system, on the other hand, is how a user accepts and agrees that using an existing model is not expensive. As a result, understanding the perceived innovation is neither difficult nor easy. In this approach, customers value a new service more than its competitors. This is due to the fact that they can quickly test the latest innovation and assess its benefits. The perception of simplicity of use is popular in the e-commerce business. Many consumers feel that their performance will improve as a result of their internet shopping. As a result, perceived ease of use is a practical factor that influences online shopping.

