International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.215-218
DOI: http://dx.doi.org/10.21172/1.101.38
e-ISSN:2278-621X

E-COMMERCE FRAUDS

Chirag[1], Ananya Mehan[2]

Abstract- Developments in information and communications technology in the last decade have significantly changed lives and provided new opportunities for consumers and businesses. An increasing number of consumers have access to the Internet and engage in e-commerce, which provides easier and faster access to products and service. It also presents some challenges for consumers that differ from those encountered during offline commercial transactions. Such challenges have given rise to the need to adapt existing legal and regulatory frameworks to the particular requirements of e-commerce. E-commerce covers a wide range of transactions effected via mobile telephones and other devices such as personal computers and tablets, and purchases are often made by using applications and platforms. Often consumers don't feel safe online and some issues need to be addresses.
E-Commerce need more security for the customers to share personal details online. In this paper, we examined the risk and measures of E-commerce Fraud.

1. INTRODUCTION

Developments in information and communications technology in the last decade have significantly changed lives and provided new opportunities for consumers and businesses. An increasing number of consumers have access to the Internet and engage in e-commerce, which provides easier and faster access to products and service. It also presents some challenges for consumers that differ from those encountered during offline commercial transactions. Such challenges have given rise to the need to adapt existing legal and regulatory frameworks to the particular requirements of e-commerce.

2. TYPES OF E-COMMERCE FRAUDS

2.1. Identity Theft

The most common type of theft is identity theft. In traditional identity theft, the criminals' goal is to carry out transactions using a different identity rather than making a new one. In order to commit identity theft, fraudsters target personal information, such as names, addresses and email addresses, as well as credit card or account information. This enables them, for example, to order items online under a false name and pay using someone else's credit card information or by debiting another person's account.

2.2 Phising

Phising is the next common types of fraud, to obtain sensitive information such as usernames, passwords and credit card details. It relies on social networking techniques applied by accessing emails, text messages or over any social media website such as Facebook and Twitter.

2.3 Pharming

Pharming is an attack in which users are redirected to fraudulent website rather than the existing site. Often the only information required is a stolen password, that can be easily found over an existing account with an online shop, where the payment data is already stored in the users account.

2.4 Friendly Fraud

In this method, customers order goods or services and pay for them using a "pull method" payment method like a credit card or debit card. After the arrival of the order they deliberately initiate a chargeback, clamming that their credit card or account details were stolen and get a reimbursement keeping the goods.

2.5 Clean Fraud

This main idea behind clean fraud is that a stolen credit card is used to make a purchase, and then manipulating in such a way that fraud detection functions are implemented. This type of fraud involves a lot of analysis of the fraud detection deployed, along with the details of owners.

[1] BE 3rd year, UIET, PU, Chandigarh
[2] BE 3rd year, UIET, PU, Chandigarh

2.6 Affilate Fraud

Affiliate fraud used to get more money form an affiliate program by manipulating traffic or signup statistics. This can be done using a fully automated process or by getting people to log into the site using fake accounts.

2.7 Triangulation Fraud

During triangulation fraud, the fraud is carried out via three points. The first is a fake online storefront, which offers high-demand goods at extremely low prices. In most cases, additional bait is added, like the information that the goods will only be shipped immediately if the goods are paid for using a credit card. The second corner of the fraud triangle involves using other stolen credit card data and the name collected to order goods at a real store and ship them to the original customer. The third point in the fraud triangle involves using the stolen credit card data to make additional purchases.

2.8 Merchant Fraud

Merchant fraud is another method where goods are offered at cheap prices, but are never shipped. The payments are, of course, kept. This method of fraud also exists in wholesale. It is not specific to any particular payment method, but this is, of course, where no-chargeback payment methods (most of the push payment types) come into their own.

Fraud methods vary depending on the sales channel, and the fact that most merchants aim to achieve multi-channel sales does not make the situation any easier. According to 69% of merchants surveyed, sales via third-party websites like Amazon, Alibaba or eBay are particularly susceptible to fraud. These are followed by mobile sales (mentioned by 64%) and sales via their own online shops (55%).

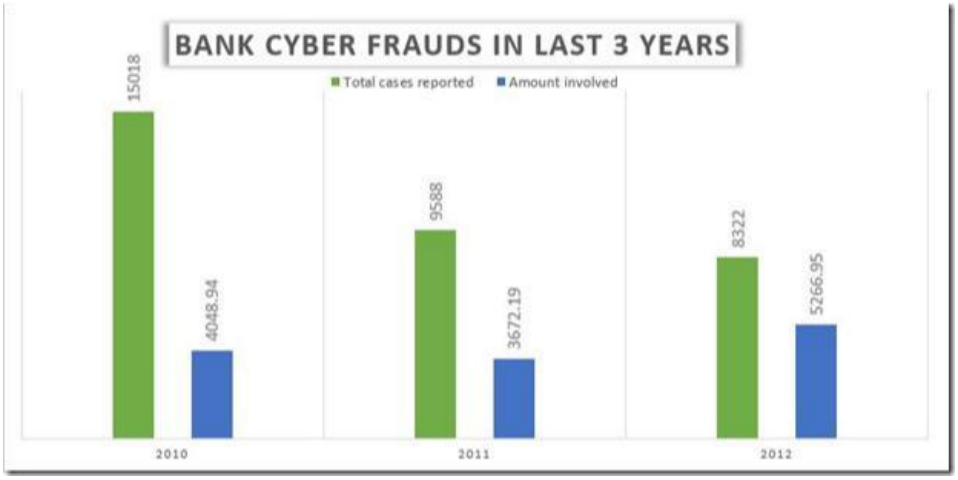

Figure 1

3. E-COMMERCE FRAUD ISSUES

3.1. Intellectual Property Issues

The contours of Intellectual Property and E-commerce are intrinsically bound with each other. Intellectual Property essentially contemplates ideas in the form of patents, copyright, trademark and design. The e-commerce platform showcases some of the intellectual property such as trademarks and designs, making brand vulnerability a concern on the online trading precinct. Brands and trademarks have been misused on the e-commerce websites and sale of counterfeit products on online websites have been ramped. For instance, in April, 2016 furniture manufacturer, Housefull International accused online market place Mebelkart of selling fake furniture under its brand name. Additionally, in 2015 Snapdeal was accused by famous Nalli Silk Sarees for misusing its brand name Nalli on its e-commerce website. Moreover, online market places like Amazon, Flipkart, and eBay have also been brought under the legal scanner for misusing brand names.

As an outcome of this it is essential to determine the liability of E-commerce websites which merely provides a platform for online transactions and in such cases getting hold of the actual concrete infringers and proving “negligence” or “actual knowledge” by the online market place becomes a complex affair.

3.2 Online Payment and Security Issues

Electronic payment mode usage has increased drastically recently having security issues associated with it. According to RBI (Reserve Bank of India) RTGS and NEFT volumes increased almost threefold between 2013 and 2016 reflecting greater adoption of the system by all segments of users. Furthermore, with increasing number of banks offering mobile banking services and driven by the growth in e-commerce and the use of mobile payment applications, the amount of mobile banking transitions has increased seven times increasing the value of transactions.

As a measure of the security issues RBI has notified all the Banks and Authorized Payment Networks about the security and risk mitigation the measures they need to take for electronic payment transactions in order to ensure that the transaction effected through such channels are safe and secure and cannot easily lead to fraudulent usage. The measures include validation checks for facilitating on-line funds transfer such as, enrolling a customer for internet/mobile banking, addition of beneficiary by the customer, generation as One Time Password(OTP) conform the payee, etc.

3.3 Consumer Protection Issues

Consumer protection is one of the major issue, as consumers don't feel safe sharing their personal information; address, name, credit card details, online to private sites. Several measures have been taken to ensure safety on the internet.

3.4 Liability of Consumer:

Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:

1. Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
2. Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working daysof receiving the communication from the bank regarding the unauthorised transaction.

3.5 Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

1. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.
2. In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1

Maximum Liability of a Customer

Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,0

3. Prevention Measures for E-Commerce Frauds

Here are some Acts that government has imposed:

a. Intermediary Liability under Information Technology Act: The Information Technology (IT) Act, 2008 covers "online market places" under the purview of "intermediary" and the Act further exempts intermediaries from liability and envisages that an intermediary shall not be liable for any third party information, data or communication and the intermediary's function is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored. However, the intermediary shall observe due diligence and

shall inform users of computer resource not to host, display, upload any information that infringes any patent, trademark, copyright or other proprietary rights.

b. The Consumer Protection Act, 1986: An Act to provide for better protection of the interests of consumers and for that purpose to make provision for the establishment of consumer councils and other authorities for the settlement of consumers' disputes and for matters connected therewith.

3.6 Measures to be taken by the consumer:

- Always check the credentials of the E-commerce website by which transaction is being made. Only shop through reputed E-commerce websites.
- Shop through those websites which have exchange, return and refund policies adequately placed.
- Trust those websites for shopping which are easily accessible through customer care numbers, so that in case of any problem you can immediately contact them.
- Once you receive the product, always check for the MRP mentioned on the product and verify if you have been charged more than MRP or not. If you have been charged more than the MRP then immediately contact the E-commerce website through the customer care number. Reputed and trusted websites on verification would immediately initiate refund.
- In case of unauthorized transaction immediately contact your Bank and register your mobile number with the Bank so that you receive SMS alert in case of any fraud immediately.

4. CONCLUSION

E-Commerces despite being a competent medium for interaction between consumer and merchant, there has been many cases of increasing fraud in the recent years. There needs to be high security and legal measures that need to be taken in order to make the consumer feel more secure online to share their personal information. In this paper we looked at the different types of fraud that take place online and what are the issues involved with it. Some feasible solutions from both the consumer and the legal side have been suggested. It is hoped that this study would help understand E-Commerce Fraud to provide better online experience.

5. REFERENCES

[1] "The Seven Types of e-Commerce Fraud."Information Age, 15 Apr. 2016, www.information-age.com/seven-types-e-commerce-fraud-explained-123461276/

[2] "What Is Pharming? - Definition from WhatIs.com." SearchSecurity, earchsecurity.techtarget.com/definition/pharming.

[3] "What Is Phishing? - Definition from WhatIs.com." SearchSecurity, searchsecurity.techtarget.com/definition/phishing.

[4] "The Consumer Protection Act, 1986." VakilNo1, 10 May 2013, www.vakilno1.com/bareacts/ consumerprotectionact/consumerprotectionact.html.

[5] "E-Commerce Fraud in India- Risk, Measures and Legal Implications." VakilNo1, 14 Dec. 2017, www.vakilno1.com/legalviews/e-commerce-fraud-india-risks-measures.html.