JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Consumer Protection in Digital World

Grishma Kanth

(Research scholar, Department of Commerce and Business Administration, ANU,

Contact no 9959409696, email – grishmakanth@gmail.com)

R. Siva Rama Prasad

(Assistant Professor, Department of Commerce and Business Administration, ANU

Contact no- 8985877089, email – raminenisivaram@yahoo.co.in)

Abstract

The digital revolution has taken the world by storm. It has completely changed the way, how people interact, work and most of all how people buy/shop. The digital world has led to a life full of comfort and ease of doing things. However, it has made us vulnerable to various malpractices and cyber threats. This paper gives an overview of the cybercrimes and business malpractices committed in the digital world. The paper also talks about the steps taken by different stakeholders to curb this menace. It also suggests what and how different stakeholders can work together to fight against them to protect the interest of the consumer.

Key words: Consumer, Cybercrime, Consumer Protection, Digital world

1. INTRODUCTION

In an ideal business environment, the customer has the utmost power. Consumer is the centre of every business and a vital part of the entire business process. Consumer is the end user in the distribution channel. The primary aim of every business is to acquire and retain its customers. All the decisions taken in the business organisation are mere extension of this policy.

However, who is a consumer? The consumer is the one who pays something to consume goods and services produced. In hindsight it may appear that consumer is just paying money in order to purchase the product/service. However, there is more to it. The consumer is not only parting away with the money but also lot of information about themselves in the process of buying the product. The information may be as simple and generic as their preferences/choices. However, at other instances the buyer might be divulging personal information like their name, address or contact details. In case the buyer is using plastic money or making online payment, he is giving away his/her crucial financial information to the business organisation.

In general, the business organisation uses this information as their databases for various purposes. The contact number or email addresses of consumers are widely used by companies for promoting their products/services. At times, it is used for pilot testing the new products before launching it fully in the market. What happens when this huge and precious information is compromised? These pose serious threat to the consumer as well as the reputation of the business organisation involved.

2. CONSUMER PROTECTION

The consumer is free to choose the product/service they want to buy. It is often quoted that consumer is the king. So why do we need to protect the interests of the consumer. The simple answer lies in the fact the devil is omnipresent. The malpractices are rampant. At times, these malpractices can cause small damages like

monetary loss or in other instances; it may cause serious damages like health hazards. So, the consumer must be protected at all costs.

The industry is going through new change. A new revolution called 4th revolution has taken place. The power of internet and interconnectivity and inter communication has enabled the businesses to grow enormously.

A report by the Internet and Mobile Association of India has revealed that India's e-commerce market reached USD 20 billion. The e-commerce has made a huge impact on most of the industries in India, the travel industry in particular. The other notable ones being the telecommunication industry, the online trading industry, etc. The government here has promoted e-commerce extensively, which is, in fact, a promotion of the e-consumer activities, mainly focusing on the delivery of services. However, the legal control still has to catch up with supply.

E-commerce being global and domestic in nature, efforts have been thoroughly made to ensure its protection. In India, the Consumer Protection Act 1986 governs the relations between consumers and the provider of services/goods. It should be noted here that no specific act regulates the online transactions. The consumer protection act has been carefully designed to muster the confidence of consumers in law and liability under this act thus arises when there is a deficiency in services or defect in goods or sometimes as the case maybe, unfair trade practices. The Consumer Protection Act specifically excludes from its ambit any service that is free of charge. Depending upon who is selling the actual goods to the consumers, liability triggers. Also, distribution of goods comes within the purview of consumer protection act. Some of the various protections under the consumer protection act on e-commerce can be listed below

- Removal of defects.
- Replacement of goods.
- Return of price in case of discrepancy.
- Discontinue any form of restrictive trade practice.

3. DIGITAL REVOLUTION AND ITS EFFECT ON BUSINESS WORLD

In recent times, the term "4th industrial revolution" has created a lot of buzz. In recent World Economic Forum, 4th industrial revolution was the focal point of entire discussion.

3rd industrial revolution is the name given to the digital revolution. The development of personal computers, internet along with information and communication technology are the main pillars of this revolution. It brought enormous changes in the ways of how consumer

4th industrial revolution is the revolution, which is blurring the lines between physical and digital world. There are mainly four design principles on which the 4th revolution industries work.

1) **Interoperability**: It is the ability of machines, devices, sensors embedded in the machines or wearables and people to connect and communicate with each other via the Internet of Things (IoT) or the Internet of People (IoP)
2) **Information transparency**: It is the ability of creating a virtual copy of the real physical world using information systems.
3) **Technical assistance**: It is the ability to assist humanity in making decisions and solving problems. It also refers to the process of performing tasks, which humans do not prefer to perform themselves for various reasons ranging from safety issues to physically exhaustive nature of the work itself.
4) **Decentralized decisions**: It is the ability of cyber physical systems to make their own decisions and to perform their tasks as autonomously as possible. In case of interferences, or conflicting goals, task is delegated to a higher authority level.

The 4th industrial revolution has caused the world to shrink even more by connecting it in every possible way. More the connected the world is, the more vulnerable the world becomes. With the ease in the flow of data and information, the security threats to the individual, organisations and society have increases manifold. With the advancements of technology, the crime rate has also advanced. Following are the few astounding facts about cybercrime.

- Globally, cybercrime was the **2nd most reported crime** in 2016.
- **U.S.** tops the list on the greatest number of data breaches reported worldwide.
- **550 million** people became victim of cybercrime in 2017.
- **Theft of Data** "accounts for **91.6 %** of chief cause of data breaches.
- On an average, an attacker resides within a network for **146 days before being detected**.
- Around **63 %** of network intrusion is the result of comprised username and password**.**
- In 2017, according to the Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported.
- There has been **350%** increase in cybercrime rate in India from 2011 to 2015.
- Maharashtra and Uttar Pradesh have the highest number of cybercrime cases registered

The above facts make it quite evident that the consumer is at huge risk. Consumer protection in such scenario is of utmost importance.

4. CYBERCRIMES AND BUSINESS MALPRACTICES IN DIGITAL ECONOMY

With the advent of digitalisation of the economy, their increased reliance on technology, and the increase in interconnectivity among different entities, may have a huge role to play in the growth of e-business but these have created infinite opportunities of various kinds of frauds and theft. Apart from the traditional crime, the digital world has opened the gates to new and deadlier crimes. With the increase in e –business the digital mediums, the fraudsters can commit crime anywhere on the global without ever being physically present at the crime scene. With the growth of e-business, internal and external perpetrators can exploit traditional vulnerabilities in seconds. The following are the crimes in widely present in digital world.

1) **Financial frauds**- The following are the most prevalent methods of committing financial frauds:
   a) **Identity theft**- A consumer who shops online has often divulge his /her personal details to the website/app. Name, address, phone number and email address and even the financial details are often stored in the e commerce websites. These data if breached can create havoc. Identity theft is one of most dreaded as commonly committed cybercrimes of the decade. The criminal gets hold of the database of the company website and uses this crucial personal information for personating someone else. Phishing and pharming are two widely used criminal methods of obtaining information. In phishing the criminals sends an email which if clicked directs you to fake website, which has been designed to look like authentic website. The naïve consumer often enters their account username and password, which is captured by the criminals. In pharming, the criminal hijacks the intended site's DNS server and because of which the consumer is directed to an imposter site. Hacking and malware are also used for committing identity theft.
   b) **Charge back fraud-** It is commonly known as friendly fraud. In this case, the criminal uses the credit card to order goods/services from an online business. Once they receive the product/services, they intimate the bank that their credit card was stolen. The bank in turns cancels the transaction in good faith. However, the company suffers a dual loss.
   c) **Clean fraud**- In this kind of frauds the fraudsters use stolen credit cards details to make purchases, but it is done in such a clean and calculative manner that the fraud detection functions are circumvented. Detail information about the rightful owner of the stolen credit cards is required so that during the payment process the fraud detection solution is fooled. Quite often, before committing clean fraud, card testing is done.
   d) **Affiliate fraud**- Affiliate frauds generally refer to any unscrupulous activity conducted to gain commissions from an affiliate marketing scheme/program. All the activities, which are explicitly forbidden under the terms and conditions of the affiliate marketing program/scheme, can be considered as affiliate fraud. Spamming, variation of the vendor's domain, parasite sites and traffic diverting fake clicks or referrals illegal transactions and site cloning are some of the few methods which scammers often use for committing affiliate frauds
   e) **Triangulation fraud**- As the name suggests, this type of fraud is executed in 3 phases. In the first phase a fake online storefront is created which normally specializes in selling high-end products are dirt-cheap prices. In the second phase, the scammers used stolen credit card information to buy these high-end products from genuine stores. In the third and final phase, the gullible customers who have fallen prey to these sites purchase these products using their money. The customer often goes for

repeat purchases and even give these sites high rating as they have received high quality products at quite
low prices. The schematic processing of this fraud makes it quite difficult to detect.

2) **Product Centric frauds** – the following are the product/service-related frauds committed by the scammers.

   a) **Wrong product –** In online shopping the description is often dubious or insufficient which can mislead the consumer. Often the product described does not serve the purpose as oppose to what was advertised. In case of intangible and digital content, the possibility of getting a wrong product is quite high**.**

   b) **Wrong endorsements**- The early adapters or influencers as the new generation calls them, often endorses the product just for their material benefit and misleads the consumers. The youngsters often fall prey to these kinds of trends and pay huge prices for the same. Health and beauty industry is plagued with this fraud.

   c) **Unsupervised repeat purchase**- There are numerous subscription business model where the repeat order is made. At times, these repeat orders are generated without the permission or notice of the consumer.

   d) **Adulteration**- This is probably the oldest business malpractice. We often come across this type of malpractices n food industry. Businessmen usually use the products, which looks similar to the original product but are available either free of cost (e.g., pebbles and stones) or at a very low cost (e.g., Brick powder, chalk powder). Adulterated product is often found in online shopping sites especially if they are offering the product at very low cost.

   e) **Inferior product**- In case of e-commerce, judging the quality of the product is often difficult. Various websites or mobile apps promise to offer various products at very low cost as compared to its offline price. Some of these sites/merchants are fraudulent and ship poor or inferior quality product to the consumer. The refund and exchange policies of these fraudulent are also deigned in such a fashion that the customer is always at the receiving end of the deal. These types of frauds are quite prevalent in electronics goods, apparel industry and in perishable products.

   f) **Weights and measures**-Just like offline mode, the online mode is full of frauds related to incorrect weights or measure. In offline mode, the merchants use specially designed balances where the weights of the product bought is often shown more than its actual weight. In case of online mode, the actual product received by the customers might be smaller or lighter in dimensions/weight of the products as described in the site. These fraudulent sites often have no exchange or refund policy because of which the consumer has to suffer the loss.

3) **Social media frauds**- the following are the frauds, which are committed on social media.

   a) **Paid reviews**- The consumer before making a purchase decision, often enquire about the product or brand or store. One of the most important influencing factors in this case is online reviews. Many online stores are now paying money to people to write good reviews about themselves thus misleading the consumer. Rival companies often pay people to write bad reviews for their competitors.

   b) **Donation frauds** - Many times we come across pictures/ messages where it is mentioned that retweeting /sharing or liking these pictures will generate a particular amount of donation to the needy. These are malware or spyware trying to get into our system and siphon out personal information.

   c) **Miscellaneous**- Harassments and photo morphing are some other forms of nuisances that internet has created.

The alarming rate of cybercrime across the nation, call for immediate remedial response. In order to curb this menace a trifecta system needs to be set up. The government, business world and consumer themselves – all three have to come together to fight this together. Each has an equal and important part to play in stalling and finally destroying the cybercrime network.

The **government, international organisation, business world** and **consumer** themselves – all have to come together to fight this together. The Quadra need to be in place to fight cybercrime, each has an equal and important part to play in stalling and finally destroying the cybercrime network.

A) Government – There has been a sudden surge in the cybercrime rates in past few years. Demonetization, rise of online banking transactions and governmental push towards a digital economy has open floodgates of cybercrime. It is time to take immediate and strong measures to curb this menace. The major steps taken by government of India to deal with cybercrime are as follows:

1) To combat the cybercrimes The **Information Technology Act, 2000** was enacted, which was majorly amended in 2008.
2) To ensure Internet security, Government of India established Computer Emergency Response Team (CERT-IN) in 2003.
3) **National Cyber Security Policy** was framed to safeguard the information, such as personal information (of web users), financial and banking information and sovereign data".
4) **CCTNS** project under national e-governance plan was created, which aims at creating nationwide network for criminal tracking and detection.
5) The Consumer Protection Bill was introduced in the Lok Sabha on August 10, 2015. The bill proposes to replace the Consumer Protection Act 1986, and this shall incorporate e-commerce. This bill seeks to widen the ambit and modernize the law on consumer protection due to changes in the market
   Although the government is doing a lot, there is a long way to go before we can actually see major results. The unreliability of internet, the undertrained staff are few aspects where government needs to focus in order to create a cybercrime free environment.

B) International organisations Many organizations are working to protect the interest of the consumers. Some of them are— Economic Cooperation and Development, International Chamber of Commerce and International Consumer Protection and Enforcement Network

Economic Cooperation and Development (OECD)*}:* The guidelines sanctioned after intense negotiation in the context of e-commerce, proved much helpful to the government, consumers, business and became practically feasible. They embraced flexibility in response to the development of age. The guidelines also achieved a benchmark for consumer protection in the online marketplace.

International Chamber of Commerce: It was in 1996, that the organization released 'guidelines on advertising and marketing on the internet'. The guidelines issued by the ICC were meant to be applied to all promotional activities like marketing and advertising on the internet. They set standards of ethical conduct to be observed by all involved in the above activities.

International Consumer Protection and Enforcement Network: The ICPEAN aims to preserve and protect the interests of the consumers all over the world. It shares information about activities taking place across borders, which may be of use to the consumers and promote their welfare to encourage global cooperation among law enforcement agencies.

C) Business organisation- Given the incremental increase in ecommerce crime, developing and investing in fraud prevention is no longer advisable – it is a necessity. Strong measures need to be taken to control this menace. Prompt actions is needed in the following aspects

1) Security settings – complex security settings and protocols needs to be in place. Regular checking of activity logs should be done and any anomaly detected should be reported and taken care of.
2) Staff- the staff should be trained in handling such vicious situations. Proper knowledge and training regarding hacking should be imparted to the employees.
3) Digital fraud prevention companies are there which can provide necessary infrastructure and support to deal with the cyber threats.

D) Consumer – Consumer cannot be the mute spectator in this scenario. Being aware of the cyber threat and its implication is essential. Government and business organisations can take initiatives to create awareness among their consumer about the cybercrimes and ways to avoid falling prey to them. However, the onus lies on the consumer to understand their rights and obligations and use them when the need arises. Here are few points, which consumers follow to protect themselves from cyber threats.

1. Use strong password and frequently change them. Do not use same password for different sites.
2. Keep all your software updated is another way to keep the problem at bay.
3. Keep your personal information private and do not give away personal information on public platforms
4. Secure your home network with a strong encryption password as well as a VPN.
5. In case of major security breaches in any sites which has your account, take proper and immediate action.
6. In case you feel that you might become a victim of a cybercrime, alert the local police or cyber police.

5. POLICY RECOMMENDATION/SUGGESTIONS:

Digital world has created a lot of distrust in minds of consumers. This poisonous environment is negatively affecting the e-commerce. The following recommendation if followed properly will create a fair-trade environment in which interest of consumer and the business organisation has equal importance.

General principles

1) Transparency and effective consumer protection system should be available to e-commerce consumers.
2) Governments along with other stakeholders should work together to determine what changes should be made to address the changing scenarios of e-commerce. Insights from information and behavioural economics should be taken into account.

Financial principles

1) If contract terms stipulate monetary remedies in the case of a consumer's breach of contract, such remedies should be proportionate to the damage likely to be caused.
2) There should be no hidden cost or misrepresentation of cost.
3) Consumer should have the right to cancel the order at any given point of time. They should have the right to reject the shipment if they wish to do so.
4) The terms and conditions of financial transaction should be made clear and easily accessible. Breakup of the cost should be made available
5) Consumer should be able to retain a complete, accurate, and durable record of the transactions in a format that is compatible to the platform /device used by the consumer.
6) In case of repeat purchase or subscription model, the consent of the consumer should be taken before making the purchase confirmation
7) Government along with other stakeholders should work towards consumer awareness among the consumers regarding their right and obligation especially in online transactions.

Advertising and Marketing Practices

1) Advertising and marketing of the products /service should be in tandem with the actual characteristics, access and usage conditions.
2) Business organisation should not omit or misrepresent facts or mislead the consumer. The features, quality name of goods/services etc. should not be deceptive.
3) Disclaimers should be made evident and unambiguous. The terms and conditions that might affect purchase decision should not be misrepresented or hidden. Information regarding warranty or after sale services should be clearly mentioned.
4) Businesses should take into account the technological limitations or special characteristics of a device or platform, while providing all necessary information
5) The information provided should be made available in such a manner, which is easy to understand and cannot be misinterpreted.
6) Endorsements used in advertising and marketing should be truthful, substantiated and reflect the opinions and actual experience of the endorsers. Any material connection between businesses and online endorsers, which might affect the weight or credibility that consumers give to an endorsement, should be clearly and conspicuously disclosed.
7) Special care should be taken towards product safety standards of the products meant for children and vulnerable or disadvantaged consumers, and others who may not have the capacity to fully understand the information with which they are presented.
8) Businesses should refrain from advertising or marketing goods/services or market, which pose an unreasonable risk to the health or safety of consumers. Businesses should co-operate with the competent authorities when a good or a service on offer is identified as presenting such a risk.

Privacy principles

1) The consumer should be made aware of the fact that their personal data is being collected for company use. The data collection should be done in lawful and fair manner.
2) Consumers should be allowed to express their view (positive or negative), file complaints or dispute charges if they wish to do so.
8) Consumer should have an option choosing whether they wish to receive unsolicited commercial text messages, e-mail or any other form of communication.
3) Business organisation should manage digital security risk and implement security measures for reducing or mitigating adverse effects relating to consumer participation in e-commerce.

Dispute redressal principles

1) Appropriate dispute resolution and grievance redress mechanism should be easily available.to the consumer.
2) Consumers should have access to Alternative dispute redressal mechanisms especially in case of low value or cross-border transactions.
3) Governments and other stakeholders should ensure that consumer protection enforcement authorities that handle consumer complaints, have the ability to take action and obtain or facilitate redress for consumers, including monetary redressal.

6. CONCLUSION

Consumer protection is always a matter of great concern. In all periods of life like ancient and medieval period, effective measures were initiated to protect consumers from crime in the market place. During British period, many laws were enacted to protect the interest of the consumers. But slowly the system was corrupted with deficiencies that discouraged the consumer from seeking legal remedy. But the government has always played a vital role in protecting consumers. Implementation of the consumer protection act reveals that, interest of consumers is better protected than before in a cost effective and timely manner.

Above all the consumers themselves have to be more aware of their rights, vigilant about unfair trade practices. Technology is leaping with unmatched speed, today. As Charles Clark once remarked, 'the answer to the machine is in the machine.' Though trade has too lived up to this and thus started off with the idea of e-commerce, however, the review of existing legal framework shows that it has failed to address the e-commerce needs. The consumer protection Act does not include any service that is free of charge in its ambit. Thus, an online transaction that does not charge the consumers clearly remains unprotected by the consumer protection act. Thus, discrepancies and loopholes pose a huge hurdle in protecting the consumers who participate in e-commerce. Here in India, the journey has commenced undoubtedly, but it is indeed a long way to go.

References

- https://en.wikipedia.org/wiki/Industry_4.0
- https://www.forbes.com/sites/jacobmorgan/2016/02/19/what-is-the-4th-industrial-revolution/#51650ee6f392
- https://en.wikipedia.org/wiki/Consumer
- https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution
- https://www.go-gulf.com/blog/cyber-crime/
- https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
- https://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276/
- https://en.wikipedia.org/wiki/Chargeback_fraud
- https://www.sec.gov/investor/alerts/socialmediaandfraud.pdf
- https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013
- https://ccgnludelhi.wordpress.com/2017/03/24/law-enforcement-initiatives-towards-tackling-cyber-crime-in-india/
- https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html
- http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf
- https://www.oecd.org/sti/consumer/toolkit-for-protecting-digital-consumers.pdf
- https://blog.ipleaders.in/consumer-protection-e-commerce/