Grant Thornton
An instinct for growth™

ASSOCHAM
INDIA

Law & Technology: Evolving challenges as a result of fraud in E-commerce sector

Contents

Foreword

In modern day India, the power of e-commerce cannot be under-emphasised. It is all pervasive in our daily lives, and we use e-commerce in various activities that vary from ordering food to buying clothes and travel. E-commerce as a sector has witnessed stupendous growth buoyed by the interests from Private Equity and Venture Capital firms which is based on the sheer consumer potential that the Indian market holds. In the process, the e-commerce firms are also moving from a startup phase to a more structured and mature phase. As a part of this journey, a number of organisations and their investors have realised that the frauds, whether done internally or by external parties, are significantly eating into their bottom line and as a result, they are becoming more sensitive to fraud risks.

Frauds in the e-commerce sector not only lead to financial loss, but also reputation loss and potential loss of business, which can be severe. In a sector such as e-commerce, where the barriers to entry are low, a fraud which can compromise customer payment information or their personal data can make the customers lose faith in the company and switch to another competitor. With an increasing regulatory enforcement and severe pressure on the bottom line, several e-commerce companies are taking a hard look at their business models and their vulnerability to fraud.

We, through this publication, argue for a proactive approach that will allow companies to address the risk of frauds in their processes, thereby strengthening their systems, processes and controls to minimise any damage resulting from such frauds. Companies need to invest in building quick response teams and asking right questions when they are hit with such instances, so they are ready to respond in an efficient and effective manner.

We are delighted to be a knowledge partner with Assocham in publishing this white paper and hope that the companies and investors are equally benefitted by this publication. Should you like to get in touch to discuss any aspect of this whitepaper, please contact us at our co-ordinates below.

Kunal Gupta
Executive Director
Grant Thornton India LLP
E: Kunal.Gupta@in.gt.com

Vidya Rajarao
Partner, National Leader, Forensic Services
Grant Thornton India LLP
E: Vidya.Rajarao@in.gt.com

Foreword

The relations between law and technology are both simple and exceedingly complex. In a world mediated by complex technologies, technological developments can undermine important interests and values that the law seeks to protect. A better understanding of the ways that the law reacts to and bring about technological change could promote more informed policy analysis. Technology is changing rapidly and our community has an increasing dependence on that technology. Therefore, it is extremely important to ensure that our laws keep up with the times.

Laws can prevent technology-enabled privacy abuses, such as intrusive surveillance or attribution of sensitive information to uniquely identifiable individuals. The interplay between law and technology is sufficient to raise serious policy questions about how that interplay can be improved. The current regime has conferred immense benefits on mankind. Yet as the discussion has shown, it is in no way optimal.

To provide a holistic outlook with good understanding of the various contemporary legal issues related to the technology Industry, **ASSOCHAM, along with Grant Thornton in India,** has come up with this study paper, to attempt to enhance the understanding of the issue related to Law & Technology.

I am sure this study will give a rich insight and adequate knowledge to all the stakeholders.

I wish the Conference a great success.

With Best Wishes,

D. S Rawat
Secretary General
ASSOCHAM

E-commerce in India

Background

Internet has become an integral part of the growing urban population segment to help them remain connected with friends, access emails on the go, buy movie tickets and order food. The changing lifestyle of the urban population has also resulted in many people relying on the internet for their shopping needs. The convenience of shopping from the comfort of one's home while having a wide product assortment to choose from has brought about an increased reliance on the online medium.

The e-commerce sector has seen unprecedented growth in past few years. This market in India has enjoyed a phenomenal growth of almost 50% over the last five years. The growth was driven by rapid technology adoption led by the increasing use of handheld devices such as smartphones and tablets, and access to the internet through broadband, 3G, etc. which led to an increase in the online consumer base. Furthermore, favoured demographics and a growing internet user base helped aid this growth.

India is expected to witness an unprecedented growth in the number of smartphone users to over 650 million in the next four years[1]. It is expected to overtake the US as the second largest market for smartphones in the world by 2016, with the growing affordability of smart mobile devices. The number of smartphone users in India is projected to exceed 200 million, ranking next to the US as the world's second largest smartphone market by 2016 due to increasing penetration of affordable smart mobile devices in the country. With the growing number of smartphone users and major e-commerce players, number of users relying on App-based platforms will eventually increase in the near future.

The number of users making online transactions has grown exponentially, and it is expected to increase from 11 million in 2011 to 38 million in 2015.

Government of India's plan to rebuild and modernise the Indian postal infrastructure and plan to implement Digital India will also affect the e-commerce sector. Both of these projects will help in increasing the reach of e-commerce players to generally non-serviceable areas, thereby boosting the growth prospects for their businesses.

E-commerce sector is set to maintain its growth trajectory driven by the stabilisation of the ecosystem and interest demonstrated by VC players, combined with support from the government.

Current Status of the e-commerce sector in India.

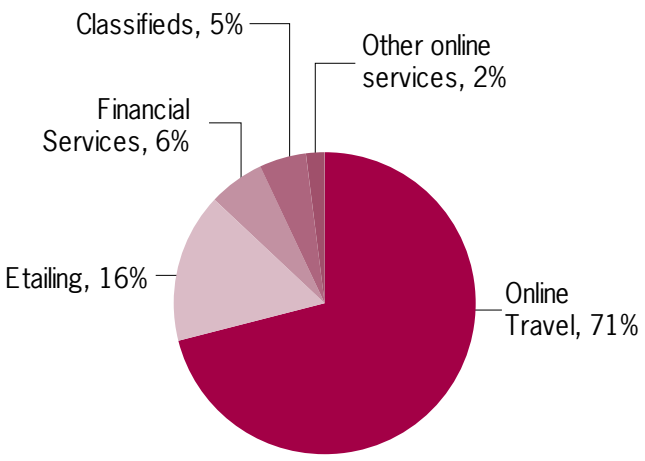
The Indian e-commerce market is estimated to grow at a Compounded Annual Growth Rate (CAGR) of 63% to reach ~USD 8.5 billion in CY 2016. Growth in the penetration levels of mobile and internet and increased consumer demand will drive this growth. India is almost 10 years behind China in the e-commerce space. China's inflection point was reached in 2005 when its size was similar to India's current market size. India's current dynamics are similar to what existed in China then – growing broadband penetration, acceptance of online marketplaces, and lack of physical retail infrastructure in many places.

Online travel dominates the Indian e-commerce market, while online travel contributes a smaller share to the global e-commerce market. Online travel accounts for nearly 71% of the e-commerce business in India. This business has grown at a CAGR of 32% between 2009 and 2013. E-tailing, on the other hand, accounts for only 8.7% of organised retail and a minuscule 0.3% of total retail sales.

Indian players, are not even thinking of profitability right now. They are focusing only on increasing their market share and market penetration.

In India, online shoppers are expected to increase from 20 million in 2013 to 40 million in 2016. An additional 200 million Indians will access the internet in the next three years, with majority of them coming online through smartphones.[2]

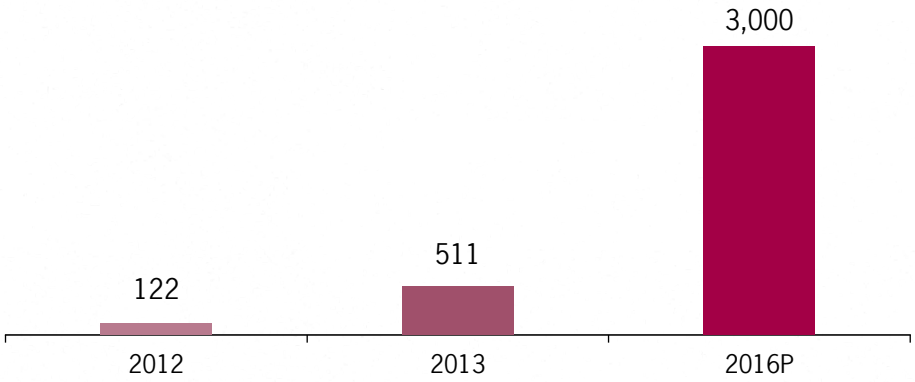
Indian Internet revenue contribution



1. Article from Indianbusiness on smartphones - http://indiainbusiness.nic.in/newdesign/index.php?param=newsdetail/10367
2. Facts and figures from various surveys and online media.

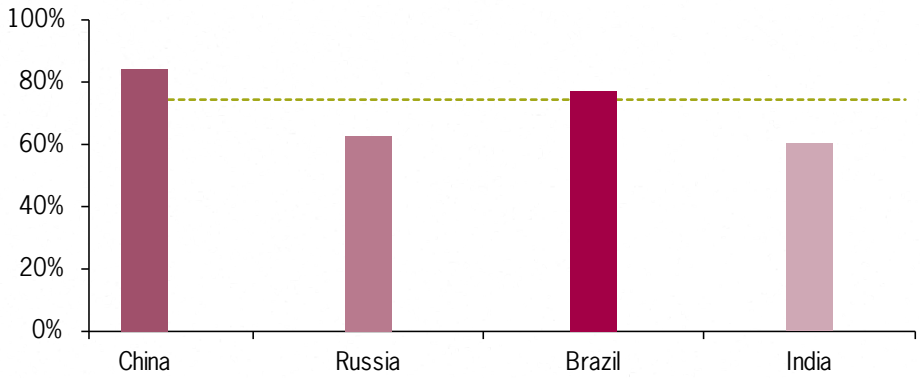
The percentage of working women in India grew 43% y-o-y in 2013, which constitutes 10% of the active online users in India. The women focused share of e-commerce market will increase from 26% in 2013 to 35% in 2016.

Women influenced e-commerce market (in $ million)



Maximum demand for online retail exists across 4,000-5,000 towns and cities in India, but there is no significant presence of physical retail in almost 95% of these locations. High real estate cost is one of the main reasons why organised retail is unable to expand at speeds expected earlier. Real estate as a percentage of sales is 14 times higher than in the US.

Reach of Online Retail Category



Around 75% of Indian internet users are in the age group of 15 to 34 years. This category shops more than the remaining population. Peer pressure, rising aspirations with career growth, and fashion trends encourage this segment to shop more than any other category and India. This category, therefore, clearly enjoys a demographic dividend that favours the growth of the India e-commerce sector.

A significantly low (19%) but fast-growing internet population of 243 million in 2014 is an indicator of the sector's huge growth potential in India. This indicates the potential of internet use in India and as internet penetration increases, the potential of growth of the e-commerce industry will also increase.

Key Players & Challenges in the e-commerce sector

Size of the Indian e-commerce sector is projected to increase from US$ 10 billion to US$ 43 billion in the next five years, according to Nomura's India Internet Report, June 2015. There are 11 categories, and within these categories, there are 42 players that are poised to shape the sector's growth trajectory.[3] According to Matrix Partners, many 'Billion dollar e-commerce companies' are expected to be created in India by 2020. At present, there are just three such companies: **Flipkart, Snapdeal and Paytm** that has just joined the club.

Tradus and BigBasket:

Tradus has recently transitioned from being a horizontal marketplace to grocery seller. While it remains a marketplace, connecting local buyers and sellers in seven cities, BigBasket is not a marketplace and therefore has more control over the entire supply chain. BigBasket has presence in four cities and has its own warehouses and delivery network.

Myntra, Jabong, Zovi and FashionandYou:

Myntra and Jabong have been in existence since 2012 and follow both inventory-led and managed marketplace models. On the other hand, Zovi designs and manufactures privately labelled lifestyle apparel and accessory products that it sells online exclusively. Lastly, FashionAndYou is a marketplace that operates in a flash sales model, offering products from retailers at discounts for only a limited period.

FirstCry, HopScotch and BabyOye:

FirstCry is a leader in babycare products online retail segment, and has been around for four years now. HopScotch is a relatively new entrant and has a flash sales model (which offers smaller scale) as opposed to FirstCry's inventory-led model. BabyOye follows both an inventory storage model and a just-in-time arrangement with its distribution partners. It appears that the niche baby care players have increasingly been edged out of the market by the large horizontal players such as Flipkart, SnapDeal and Amazon.

UrbanLadder, FabFurnish and PepperFry:

UrbanLadder is a curated online marketplace for furniture and home decor products. FabFurnish too is shifting from an inventory-led model to a marketplace model, thus becoming more cost-effective and also covering more cities. Pepperfry is a managed marketplace that switched focus from initially selling products across multiple lifestyle categories to only furniture and home décor. It has the largest coverage, shipping to about 500 cities in India.

3. Article in economic times related to trends and future prospects of e-commerce.

Challenges

Though this sector has experienced a phenomenal growth and it excites entrepreneurs and financial investors alike, some serious challenges are beginning to weigh down on the sector.

We will focus on some key challenges that e-commerce sector is facing or might face in the near future.

1. E-commerce in India has many first-time buyers. Companies need to address issues pertaining to rapidly evolving customer segments and product portfolios like accessibility of market intelligence on growth, size and share; focus on expansion into new geographies, brands and products; and simultaneously tackle a hypercompetitive pricing environment. With the increasing challenge and entry of new players in the market, companies have to provide a rich, fresh and simple customer experience, manage inconsistent brand experience across platforms and handle time-to-market pressure for new applications. In the recent past, social media has become more influential than paid marketing.
2. Low credit card penetration and low trust in online transactions has led to cash on delivery being the preferred payment option in India. Unlike electronic payments, manual cash collection is laborious, risky, and expensive. Also, payment gateways have a very high failure rate. E-commerce companies using Indian payment gateways are losing out on business, as several customers do not reattempt payment after a transaction fails.
3. In India, there is little standardisation in the way postal addresses are written. Last mile issues add to e-commerce logistics problem. The logistics challenge in India is not just about the lack of standardisation in postal addresses. Given the large size of the country, there are thousands of towns that are not easily accessible. Metropolitan cities and other major urban centers have a fairly robust logistics infrastructure. But since the real charm of the Indian market lies in its large population, absence of seamless access to a significant proportion of prospective customers is a dampener.
4. Internet penetration is still very low in India. It is still a small fraction of what one would find in several western countries. Also, even if all the infrastructure and integration issues are fixed, illiterate citizens may be unable to transact directly on e-commerce sites that require reading and writing skills.
5. E-commerce in India could be very profitable; it will just take time and effort. Leaders of the country need to understand that besides websites, there are many other elements which entrepreneurs need to consider to ensure the success of their ventures. These include investing in infrastructure like postal system, broadband, and transportation networks; setting up a pan-India system to prosecute fraud and improve business trust in internet; and most importantly, improving literacy rates. To make the web infrastructure work for businesses, leaders need to focus less on how to improve the number of total domains registered and instead fix the physical business ecosystem which they continue to neglect in order to unleash the wealth-creating powers of the web in India.[4]

Cloud computing and Challenges –

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud was inspired by the symbol that's often used to represent the Internet in flowcharts and diagrams. Cloud computing enables companies to consume compute resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house.

Cloud computing is a general term for the delivery of hosted services over the Internet. Cloud computing enables companies to consume compute resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house.[5]

4. Article in Harvard Business Review related to challenges in e-commerce in Africa.
5. Article from TechTarget.com - http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Following are the challenges and the risks that are worth considerable:

1. Privacy agreement and service level agreement
2. Security and data protection
3. Location of data
4. Legislation and regulation

Intellectual property and related issues

A company's website can be a great tool for promoting business online and for generating sales. However, as Web commerce increases, so does the risk that others may copy the look and feel of your website, some of its features or the content on your website. The risk also increases that you may be accused of unauthorized use of other people's intellectual assets. The battle against counterfeiting and work on IRP protection could be a drawn-out process.

For almost every e-commerce operator today, its e-commerce business is no longer a neutral vehicle engaged solely in the technical processing of data. Every operator takes initiatives to build up their relations with users, exerting control over the user's data, either public or private, and providing assistance in promoting users' sales. Providing these value-added services is definitely the future of the e-commerce business model in this fiercely competitive market. Unfortunately, this business model will also lead to high legal risks if the operators do not figure out clearly how to deal with possible IP infringers on their platforms.

E-commerce operators are advised to:

1. Be ready for responsibility: Be prepared to take on more responsibilities when it comes to the IP protection of brand owners. This is particularly pertinent where e-commerce providers are actively involved in the services it offers to its users.
2. Conduct a self-investigation and analysis: Conducting an investigation on your own business model and analyse whether you have played an active role in promoting services that have a high risk for IP infringement.
3. Establish a supervision system: Set strict market access for users who are your potential "active role" service acceptors.
4. Collaborate with brand owners: Collaborate with brand owners to jointly survey for IP infringement activity and share this cost.
5. Employ public relations: Avoid being misjudged as a counterfeiting platform by engaging in appropriate public relations.[6]

Consumer Data protection

Most companies are in possession of vast amounts of data about employees, consumers and their own products and activities. To protect these interests and their reputation, as well as to comply with regulations, business entities must do all they can to prevent breaches. These can come in many forms – databases being sold or hacked into, carelessness on the part of employees with access to sensitive data or the misuse of data intended for other purposes. All of these can result in high-profile negative press coverage or in punishments by regulators, and as companies handle more and more data (the inevitable result of the production of online content and activities by individuals, which are stored in perpetuity) the rate of incidence of breaches looks set to continue to grow.

Perhaps the most challenging aspect of working in internet, technology or IT law is keeping up with the development of new technology and regulations. Many clients in these industry sectors have a particular business culture and way of working that emphasises innovation and their lawyers have a need to keep up with and understand this.

Staying abreast of technological developments is not only important within the context of the relationship with the client who has developed it – doing this can also have a beneficial effect on the quality of legal service provided to other clients. As new technologies are developed and launched, the dissemination of knowledge about them spreads. [7]

6. Article from Mondaq - http://www.mondaq.com/x/158678/IT+Internet/IP+reshapes+ecommerce+strategies
7. Article from Whoswholegal - http://whoswholegal.com/news/analysis/article/28694/research-trends-conclusions-internet-e-commerce-data-protection-2010/

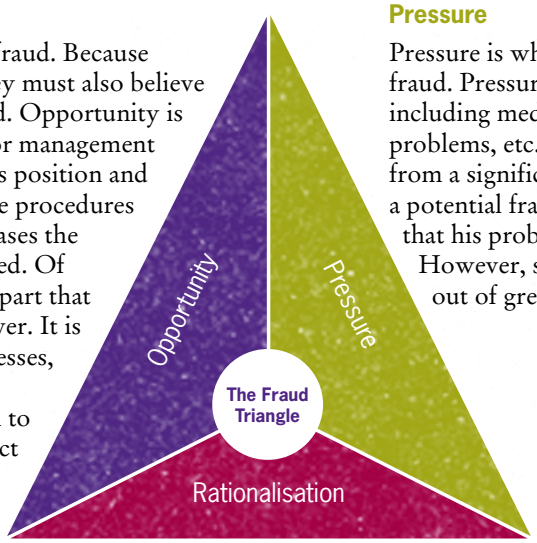
Fraud in the e-commerce sector

Traditional concepts of fraud

Corporate fraud is an ongoing reality. Fraud is often explained in terms of the fraud triangle which describes that fraud is most likely to occur when there is an overlap of an incentive or pressure to commit fraud, the opportunity to commit fraud, and a rationalisation therefore.[8]

Opportunity

Opportunity is the ability to commit fraud. Because fraudsters don't wish to be caught, they must also believe that their activities will not be detected. Opportunity is created by weak internal controls, poor management oversight, and/ or through use of one's position and authority. Failure to establish adequate procedures to detect fraudulent activity also increases the opportunities for fraud to be committed. Of the three elements, opportunity is the part that organisations have the most control over. It is essential that organisations build processes, procedures and controls that don't needlessly put employees in a position to commit fraud and that effectively detect fraudulent activity if it occurs.



Pressure

Pressure is what causes a person to commit fraud. Pressure can include almost anything including medical bills, expensive tastes, addiction problems, etc. Most of the time, pressure comes from a significant financial need/ problem.. Often, a potential fraudster believes, for whatever reason, that his problem must be solved in secret. However, some frauds are committed simply out of greed.

Rationalisation

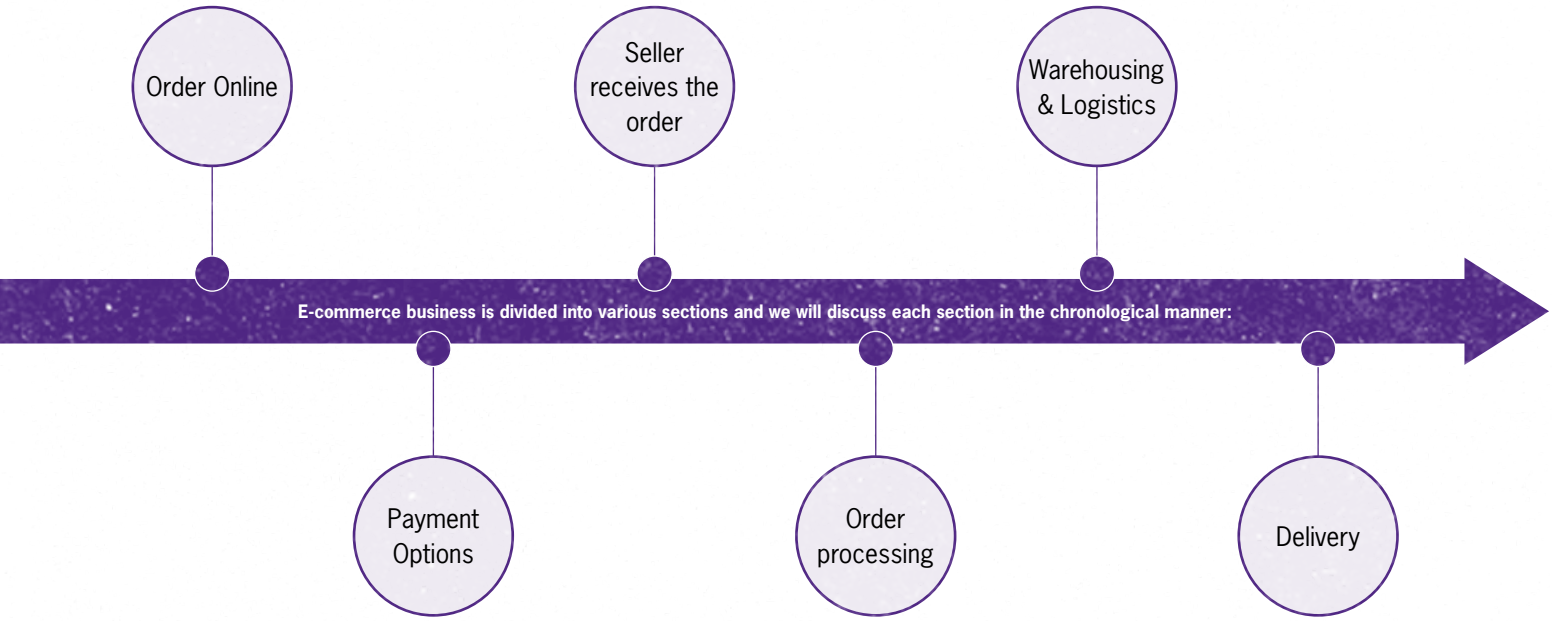
Rationalisation is a crucial component in most frauds which prompts a person to reconcile his/her behaviour (stealing) with the commonly accepted notions of decency and trust. Some common rationalisations for committing fraud are:

- The person believes that committing fraud is justified to save a family member or loved one;
- The person believes they will lose everything – family, home, car, etc. if they don't take the money;
- The person believes that no help is available from outside;
- The person labels the theft as "borrowing", and fully intends to pay the stolen money back at some point;
- The person, because of job dissatisfaction (salaries, job environment, treatment by managers, etc.), believes that something is owed to him/ her;
- The person is unable to understand or does not care about the consequence of his/ her actions or of accepted notions of decency and trust.

8. Fraud Triangle concept from Association of certified fraud examiners

Fraud challenges unique for e-commerce companies

The economic crisis has forced retailers, like other organisations, to closely examine every aspect of their business for inefficiencies. This investigation has exposed the holes that exist in their e-commerce operations. Retailers are waking up to the realities of e-commerce fraud and are realising the inadequacies of their current fraud management processes. Fraud is fast becoming an area of concern for retailers as they gear up for further growth in online commerce.



- Customer tries to order a book online. His/ her Web browser communicates back-and-forth over the Internet with a Web server that manages the store's website
- The Web server sends order to the order manager. This is a central computer that sees orders through every stage of processing from submission to dispatch
- The order manager continues to process it. Next it communicates with a merchant system (run by a credit-card processing firm or linked to a bank) to take payment using the customer's credit or debit card number
- The order manager sends a request to the warehouse to dispatch the goods to the customer.
- A vehicle from a dispatch firm collects the goods from the warehouse and delivers them.
- The goods are delivered to the customer

As the popularity of internet shopping and online auctions grows, so does the number of complaints about transactions. Some of the most common complaints involve:

- Buyers receiving goods late, or not at all
- Sellers not receiving payment
- Buyers receiving goods that are either less valuable than those advertised or significantly different from the original description
- Failure to disclose relevant information about a product or the terms of sale

There are several avenues of risk associated with each and every process. From a risk perspective, e-commerce companies could face issues around brand risk, insider threats and website uptime. Issues around employee-vendor nexus, bribery and corruption make companies vulnerable to fines. Cyber security also raises some concerns around website exploitation by external entities.

We will highlight some unique fraud challenges that e-commerce sector faces in the current scenario:

Inadequate Toolset

Typically, retail e-commerce fraud management techniques have relied on front-end payment card validations (MOD 10 checks, BIN checks, authorisation responses, etc.), customer profile checks (security questions, login analysis, etc.), or basic site rules (number of orders placed through one account, value of orders, etc.) or back-end manual order reviews. Transaction monitoring systems have been implemented, but these have been home-grown and have not kept pace with changes in the fraud domain. Some investments have been made in automatic fraud detection, but manual review processes remain the norm.

Insufficient knowledge and experience

Another fallout from the economic downturn is that the across the board headcount reduction, many retailers have enacted to contain costs. Since fraud management is not considered core to e-commerce operations, fraud management teams in many companies have been radically reduced, causing significant shrinkage of domain knowledge and bandwidth. As a result, existing teams are finding it challenging to simultaneously work on analysing and preventing current fraud schemes, while keeping up with the pace of change in the fraud domain and formulating robust strategies for detection and prevention.

Information silos

Lack of adequate focus on fraud management over the years has resulted in a lack of proper development of and integration between internal IT systems that can quickly provide data on fraud in a way that can help in swift action. Often, retailers do not have the right data readily available to measure their current fraud levels because there is no enterprise-wide view of fraud available. Creating these insights requires significant IT investments that are, again, in limited supply, given the current economic conditions.

Losses as a result of fraud

Fraud can have a substantial impact on a business, no matter what size it is. Many businesses are feeling the effects of the economic downturn and in their attempts to minimise losses, often they unknowingly open themselves to huge financial and reputational risks. This is due to the fact that when companies cut back on costs, they often increase their chances of being victims of fraud.

We will categorise losses into the following categories:

Financial loss

Financial loss is an obvious effect of both types of fraud. When someone misappropriates company assets, the loss is fairly easy to quantify. The costs of fraudulent financial reporting are harder to determine. If a business owner perpetrates financial statement fraud, an explicit dollar figure might not be obvious. However, fines assessed for misleading investors, civil suits to recoup investor and creditor losses and the unwillingness of companies to extend credit to the business in the future all add up to a severe financial loss for the company.

In most instances, actual or attempted payments fraud has resulted in relatively small financial losses. For 39% of organisations, the potential loss from fraud is estimated at less than US$ 25,000, while for 37% of organisations, the potential loss is between US$ 25,000 and US$ 249,999. The potential loss is US$ 250,000 or more for 17% of organisations.[9]

External confidence

Once a fraud has been uncovered, the company faces an ongoing problem of public trust in the organisation. While a business scandalised by fraud might never be the victim or perpetrator of another fraud, its public image might be irreparably tainted. As a consequence, the company may have to pay a higher price for credit, may be refused membership in trade associations or might not be considered for a strategic alliance.

Increased audit costs

Businesses that are subject to audit and have experienced fraud, especially if the fraud was perpetrated by the company management, are likely to be assessed as a high audit risk. That means auditors will scrutinise company books more closely before signing off on its financial statements. When an auditor is required to perform more procedures, the cost of the audit will increase. This can often be mitigated by demonstrating that the offending managers or employees have left the company and the company has instituted strict procedures to thwart future attempts at fraud.

Company morale

The effect of fraud on a company's culture and morale can be shattering. Any association with a company that has perpetrated or suffered fraud can be troubling and embarrassing for the people who work there. This may be especially true in a growing business setting where workers feel more connected with one another. Even if employees leave the company, they may carry an association with a fraudulent company into their next place of employment, even if they were not involved with the fraud at all.

9. Data from JP Morgan Fraud Survey result 2014

Legislative & other changes

E- commerce companies have to comply with several laws, many of which are still evolving.

Issues around cyber law compliance, inefficient anti-corruption framework, legal exposure in agreements or arrangements, indirect and direct tax compliance framework and Foreign Exchange Management Act, 1999 (FEMA) contraventions and regularisation could pose problems. Also, uncertainty around Value Added Tax (VAT) implications in different states due to peculiar business models could cause issues.

E-commerce laws and regulations in India are still evolving. This has created some confusion and uncertainty among e-commerce companies in India. While some have opened e-commerce outlets through websites, others are exploring a more appropriate and legal way of running an e-commerce business in India.

There are numerous legal formalities that are required to start a business entity and conduct e-commerce activity through it in India. A business can be operated as:

a. Sole Proprietorship

b. Partnership

c. Limited Liability Partnerships (LLP)

d. Company

Some of the regulations with which e-commerce companies need to abide and are relevant from the perspective of fraud monitoring are:

01 Companies Act, 2013 (2013 Act)

It is pertinent to draw attention to the definition of "foreign company" under the recently enacted 2013 Act:

As per Section 2 (42), "foreign company" means any company or body corporate incorporated outside India which:

a. Has a place of business in India whether by itself or through an agent, physically or through electronic mode; and

b. Conducts any business activity in India in any other manner.

Further, Chapter XXII of the 2013 Act contains provisions to be complied with by foreign companies not only under the 2013 Act but also under the provisions prescribed through Rules therein. The definition recognises, establishment of a place of business through the 'electronic mode. However, there is still a lack of any implicit or explicit detailing in this regard.

Also, if a company is a listed company, these companies will have to comply with the following provisions of the 2013 Act:

a. **Audit Committee requirement --** The listed companies shall be required to have an audit committee and such audit committee shall consist of minimum three directors with independent directors forming a majority. While Section 149 (4) of the 2013 Act does not prescribe for a need for an independent director but pursuant to this section will require independent directors (Section 177). In the Companies Act, 1956 (1956 Act), only public companies, but not private companies, were required to have an audit committee.

b. **Nomination and Remuneration Committee requirement --** Listed companies will be required to have a nomination and remuneration committee as well, comprising three or more non-executive directors, out of which, no less than one-half need to be independent (Section 178).

c. **Secretarial Audit --** Though the section specifies secretarial audit for bigger companies; all listed companies are required to provide for a secretarial audit report along with the board's report which shall be duly signed by the company secretary in practice (Section 204). The PCS has to confirm that the company has complied with the provisions of several regulations from the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Securities Contracts (Regulation) Act (SCRA), listing agreement, depositories, Foreign Exchange Management Act (FEMA) and competition, to name a few.

d. **Vigil Mechanism --** Listed companies need to establish a vigil mechanism for directors and employees to report genuine concerns in such matters as may be prescribed (Section 177 (9)).

e. **Appointment of auditors --** Listed companies cannot appoint an individual as an auditor for more than one term of five consecutive years and an audit firm as auditor for more than two terms of five consecutive years. There shall be a cooling off period for the individual auditor and the audit company for a period of five years after their expiry of term mentioned above. Then one cannot appoint an audit firm whose partner or partners are common to other audit firm whose tenure expired (Section 139(2)).[10]

10. Publication from ICSI on Companies Act 2013

02 Information Technology Act, 2000 (IT Act 2000)

In India, e-commerce received a tremendous fillip and boost thanks to the passing of the IT Act 2000. In fact, the Indian Information Technology Act, 2000 is an e-commerce enabling legislation as it provided a legal framework for e-commerce to really take off in the year 2000.

The IT Act 2000 has also provided the solid basis and foundation for further growth of e-commerce and m-commerce. The IT Act 2000 was amended by the Information Technology (Amendment) Act, 2008. This expanded the scope and ambit of the IT Act 2000 to include all kinds of communication devices and computer resources. The said amendments came into effect on 27 October 2009 and provided a legal enabling framework for the growth of mobile commerce, which formed part of the e-commerce sector.

The government has further sought to provide far more exhaustive coverage of cybercrimes in the law. Various new cybercrimes have been added like the activities defined in Section 43 of the IT Act 2000.

Section 79 of the IT Act 2000 has been amended to address the concerns of corporates. The new law has clarified that intermediaries including network service providers shall not liable for any third party data or information made available by them as a general principle and some exceptions to the rule have been stipulated.

However it needs to be noted that the IT Act 2000 was enacted in the year 2000 and was only amended once in 2008. However, a lot of new developments have taken place in the field of technology and there is a need for updating the law so as to keep it in sync with the realities of today's times.

The IT Act 2000 also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the government at a later date.

The increased use of the internet has led to a virtual world which is not possible to be restricted in terms of traditional concepts of territory, which has led to complications in determining jurisdiction. According to the traditional rules of jurisdiction determination, the courts in a country have jurisdiction over individuals who are within the country and/or over the transactions and events that occur within the natural borders of the nation.

Therefore in e-commerce transactions, if a business derives customers from a particular country as a result of their website, it may be required to defend any litigation that may result in that country.[11]

IT Act 2000 contains a provision which provides for such long arm jurisdiction:

Section 1(2) of the IT Act 2000 read along with Section 75 of the IT Act 2000 provides that:

- The IT Act 2000 shall extend to the whole of India and, save as otherwise provided under the IT Act 2000, it shall also apply to any or contravention thereunder committed outside India by any person; and
- The IT Act 2000 shall apply to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

11. Article by Nishith Desai & Associates on e-commerce.

Indian Penal Code (IPC)

Obscenity - Any material which is lascivious or appeals to the prurient interest or which may deprave and corrupt persons would be considered obscene and publicly exhibiting such obscene material (which may include posting on a website) would attract liability under Section 292 of the IPC. Liability could be in the form of imprisonment and fine. Further, increased liability is attracted when such obscene material is made available to young people. In fact, the wide accessibility to internet by persons of all age groups may make it difficult to prove that any material considered obscene was not made available to young people.

Jurisdiction - Section 3 of the IPC provides that any person who is liable, by any Indian law, to be tried for an offence committed outside India shall be dealt with in accordance with the provisions of the IPC for any act committed beyond India in the same manner as if such act had been committed within India.

There does not seem too much jurisprudence in India on the issue of jurisdiction in cases of e-commerce.

03 CBI, SFIO & other agencies

Serious Fraud Investigation Office (SFIO) – A part of the Ministry of Corporate Affairs (MCA), SFIO is involved in major fraud probes and is the coordinating agency with the Income Tax department and the Central Bureau of Investigation (CBI). It comprises experts from various organisations like banks, Securities & Exchange Board of India, Comptroller and Auditor General and concerned organisations and departments of the government.

The SFIO does not initiate any investigation on its own, based on any complaints/documents received from any source. The cases are taken up for investigation as are ordered for investigation by the government i.e. MCA under Section 235, 237, 239 and 247 of the 1956 Act. Thus, keeping in mind the limited powers offered to the SFIO under the provisions of the 1956 Act, the 2013 Act has made SFIO statutory authority to strengthen its power & responsibilities relating to investigation. Section 447 of the 2013 Act provides provision of punishment in case of fraud.

Some reports submitted by SFIO includes one of major sportswear maker Reebok India for violations by the Indian as well as overseas management personnel on the allegations of financial irregularities and Saradha Chit fund scam for financial mismanagement and siphoning off funds by their promoters.[12]

Central Bureau of Investigations CBI

India's first agency to investigate corruption, the Special Police Establishment, was set up in 1941 – six years before the country's independence from British rule – to probe bribery and corruption in the country during World War II. That agency was part of India's War Department. In 1946, it was brought under the Home Department and its remit was expanded to investigate corruption in Central and State governments under the Delhi Special Police Establishment Act.

To begin an investigation, the agency must obtain a series of approvals. For corruption investigations, which are monitored by the Central Vigilance Commision (CVC), the CBI needs the approval of the Personnel Ministry, and from the Chief Minister of the State where it wants to conduct an investigation.

The following broad categories of criminal cases are handled by the CBI:

- Cases of corruption and fraud committed by public servants of all Central government departments, Central public sector undertakings and Central financial institutions.
- Economic crimes, including bank frauds, financial frauds, import export & foreign exchange violations, large-scale smuggling of narcotics, antiques, cultural property and smuggling of other contraband items, etc.
- Special crimes, such as cases of terrorism, bomb blasts, sensational homicides, kidnapping for ransom and crimes committed by the mafia/ underworld.[13]

12. Facts & Figures used from Assocham's article on SFIO.
13. CBI Website

What companies can do to prevent fraud

The sustained growth of the e-commerce sector continues to attract criminals who continuously develop new schemes to defraud merchants and their customers. These cyber thieves persist in devising increasingly sophisticated ways to steal personal account information from merchants, and to accumulate goods, services, and quasi-cash through unauthorised use of that information at merchant Web sites.

For the organisation's fraud risks to be effectively managed, they must first be identified using a formal risk assessment process. If performed and used correctly, a fraud risk assessment can be a powerful proactive tool in the fight against fraud for any business.

Controls

We can categorise our fraud prevention controls into two categories:

- **Preventive controls**
- **Detective Controls**

Preventive controls are intended to prevent fraud before it occurs, and include:

- Bringing awareness to personnel throughout the organisation on the fraud risk management program in place
- Performing background checks on the employees
- Conducting exit interviews
- Implementing policies and procedures
- Segregating duties and tasks by ensuring proper alignment between an individual authority and his/ her level of responsibility
- Reviewing third party and related party transactions and relations

Detective controls are intended to detect fraud when it occurs. These include:

- Implementing proactive controls for the fraud detection process, such as independent reconciliations, reviews, physical inspections/ counts, analysis and audits
- Implementing proactive fraud detection procedures, such as data analysis and continuous auditing techniques
- Establishing and marketing the presence of a confidential reporting system, such as whistleblower hotline

Investigation

The objective of an investigation is to get the facts so that resolution of the complaint and situation can be achieved. Fraud investigations are not like standard police-type investigations concerning any criminal activity. This is because the majority of fraud investigations begin only with a mere suspicion that a fraud has occurred. In many cases, there is little initial evidence of that fraud, as the nature of most fraud is such that deception is involved in committing and then covering up the crime.

Fraud investigation resources generally fall into four categories or skill-sets. In the majority of cases, most if not all of them are required to fully investigate a suspected fraud:

- **Forensic accounting/ transaction analysis**

  Forensic accountants are responsible for quantifying and evidencing identified fraudulent transactions. This can be a challenge in situations where the suspects themselves are skilled accountants and have knowledge of the financial system. Often, a forensic accountant will need to piece together incomplete or deliberately falsified financial records.

  Forensic accountants may also be required to calculate losses and damages and prepare insurance claims..

- **Investigative intelligence and analysis**

  This is the research component of the investigation. It involves experts in publicly sourced information obtaining relevant information concerning individuals and entities suspected of involvement in the fraud. This is one of the first steps taken in an investigation where the suspect has been identified.

- **Computer forensics**

  Computer forensics involves the search, seizure and analysis of electronic evidence, which is most often found on personal computers but can also be found on virtually any modern electronic device. It is rare for modern day frauds to be perpetrated without the involvement of computers, and therefore computer forensics is a vital skill-set in the vast majority of fraud investigations.

- **Fieldwork and interviews**

  Again a crucial part of most investigations, interviews with witnesses and suspects can prove vital to an investigation. Statements made during an interview can become admissible evidence, if obtained in an appropriate manner.

Risk Management

Risk management involves identification, prioritisation, treatment and monitoring of the risks that threaten an organisation's ability to provide value to its stakeholders, such as increasing profitability and shareholder value for a for-profit entity or achieving program specific goals for a non-profit or governmental agency. More specifically, risk management balances risk appetite – how much risk the management is willing to accept – with the ability to meet the organisation's strategic, operational, reporting, and compliance objectives.

Every organisation faces a unique set of risks based upon its industry, financial condition, regulatory environment, culture, and a host of other factors. Consequently, an entity's risk management program must be tailored to the specifics of the organisation for it to be effective. Nevertheless, an established risk management framework can be very helpful in providing guidance and structure in developing such a program.

The key to reducing this vulnerability is to be consciously aware of and realistic about the organisation's weaknesses. Only then can the management establish mechanisms that effectively prevent or detect fraudulent activities. In fact, it is those organisations that deny the true possibility of fraud which are placing themselves at the greater risks.

In addition to the financial benefits, effective fraud risk management:

- Sends a clear message that the fraudulent actions will be proactively sought out and will not be tolerated
- Demonstrates a sound business strategy to employees and third parties
- Enhances the organisation's public image and reputation
- Promotes goodwill with other organisations and the general public

Even the most honest and trusted employees can one day become dishonest. Lives change, needs change, situations change, and rationalisations change. Effective fraud risk management is a continuous process of reviewing and addressing the significant risks of fraud.

About Grant Thornton

Grant Thornton International Ltd.

Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice. Proactive teams, led by approachable partners in these firms, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions. More than 40,000 Grant Thornton people, across over 130 countries, are focused on making a difference to clients, colleagues and the communities in which we live and work.

Grant Thornton in India

Grant Thornton in India is one of the largest assurance, tax, and advisory firms in India. With over 2,000 professional staff across 13 offices, the firm provides robust compliance services and growth navigation solutions on complex business and financial matters through focused practice groups. The firm has extensive experience across a range of industries, market segments, and geographical corridors. It is on a fast-track to becoming the best growth advisor to dynamic Indian businesses with global ambitions. With shorter decision-making chains, more senior personnel involvement, and empowered client service teams, the firm is able to operate in a coordinated way and respond with agility.

Over the years, Grant Thornton in India has added lateral talent across service lines and has developed a host of specialist services such as Corporate Finance, Governance, Risk & Operations, and Forensic & Investigation. The firm's strong Subject Matter Expertise (SME) focus not only enhances the reach but also helps deliver bespoke solutions tailored to the needs of its clients.

About ASSOCHAM

ASSOCHAM

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organisations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys – yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons us calling each member of the chamber to serve the nation and make a difference.

ASSOCHAM Offices

The Associated Chambers of Commerce and Industry of India (ASSOCHAM)
5 Sardar Patel Marg, Chankyapuri, New Delhi – 110021
Tel: 46550555(Hunting Line) Fax: 011-23017008/9 Website: www.assocham.org

Southern Regional Office
D-13, D-14, D Block, Brigade MM,
1st Floor, 7th Block, Jayanagar,
K R Road, Bangalore – 560070
Telephone: 080-40943251-53
Fax : 080-41256629
E-mail: events.south@assocham.com,
events@assocham.com, director.south@assocham.com

ASSOCHAM Western Regional Office
4th Floor, Heritage Tower,
Bh. Visnagar Bank, Ashram Road,
Usmanpura, Ahmedabad-380 014
Tel: + 91-79- 2754 1728 / 29, 2754 1867
Fax: + 91-79-30006352
Email: assocham.ahd1@assocham.com
assocham.ahd2@assocham.com

Eastern Regional Office
F 4, "Maurya Centre" 48, Gariahat Road Kolkata-700019
Telephone: 91-33-4005 3845/41
Fax: 91-33-4000 1149
E-mail: kolkata@assocham.com

ASSOCHAM Regional Office Ranchi
503/D, Mandir Marg-C
Ashok Nagar
Ranchi-834 002
Email: Head.RORanchi@assocham.com
Phone: 09835040255

Contact us

To know more about Grant Thornton in India, please visit **www.grantthornton.in** or contact any of our offices as mentioned below:

NEW DELHI
National Office
Outer Circle
L 41 Connaught Circus
New Delhi 110001
T +91 11 4278 7070

AHMEDABAD
BSQUARE Managed Offices
7th Floor, Shree Krishna Centre
Nr. Mithakali Six Roads
Navrangpura
Ahmedabad 380009
T +91 76000 01620

BENGALURU
"Wings", 1st Floor
16/1 Cambridge Road
Ulsoor
Bengaluru 560008
T +91 80 4243 0700

CHANDIGARH
B-406A, 4th Floor
L&T Elante Office Building
Industrial Area Phase I
Chandigarh 160002
T +91 172 4338 000

CHENNAI
Arihant Nitco Park, 6th Floor
No.90, Dr. Radhakrishnan Salai
Mylapore
Chennai 600004
T +91 44 4294 0000

GURGAON
21st Floor, DLF Square
Jacaranda Marg
DLF Phase II
Gurgaon 122002
T +91 124 462 8000

HYDERABAD
7th Floor, Block III
White House
Kundan Bagh, Begumpet
Hyderabad 500016
T +91 40 6630 8200

KOCHI
7th Floor, Modayil Centre point
Warriam road junction
M.G.Road
Kochi 682016
T +91 484 406 4541

KOLKATA
10C Hungerford Street
5th Floor
Kolkata 700017
T +91 33 4050 8000

MUMBAI
16th Floor, Tower II
Indiabulls Finance Centre
SB Marg, Elphinstone (W)
Mumbai 400013
T +91 22 6626 2600

MUMBAI
9th Floor, Classic Pentagon
Nr Bisleri factory, Western Express Highway
Andheri (E)
Mumbai 400099
T +91 22 6176 7800

NOIDA
Plot No. 19A, 7th Floor
Sector – 16A
Noida 201301
T +91 120 7109 001

PUNE
401 Century Arcade
Narangi Baug Road
Off Boat Club Road
Pune 411001
T +91 20 4105 7000

For more information or for any queries, write to us at **contact@in.gt.com**

Follow us **@GrantThorntonIN**