

Deloitte.

Beyond the growth story
Mitigating fraud risks in
the e-commerce industry

Private and confidential

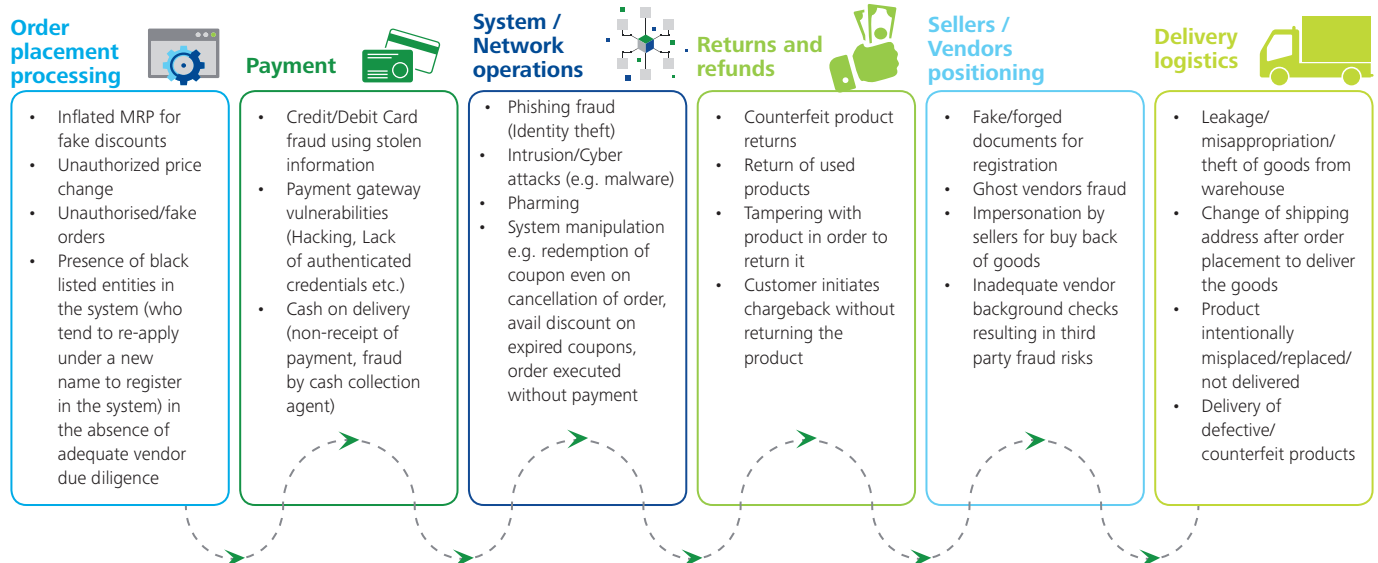


The e-commerce industry in India

E-commerce is one of the fastest growing sectors in India today, adding 6 million new entrants every month, supported by a growing internet user base¹. With such a growth pace, the e-commerce industry is projected to touch around USD 10–20 billion by 2017-2020².

The e-commerce industry, in its present form, is a complex ecosystem. It involves large volumes of transactions, reliance on newer technologies such as mobile wallets for payments and mobile apps for customer access, and dependence on third-party vendors for product procurement and logistics. Over time, the fraud risks, including phishing, identity theft related to payment systems and third-party fraud risks in procurement and logistics, such as counterfeiting, bribery and corruption etc., have started collectively impacting e-commerce businesses. In addition, with fierce competition to gain market share through aggressive pricing strategies, such as deep discounting, meeting profitability expectations of investors and the race to seek funds for expansion, the e-commerce companies may be forced to overlook their back-end processes and controls, thereby increasing the risk of frauds.

An illustrative fraud-risk landscape of an e-commerce market place company is indicated below:



¹As of June 2015, India is reported to have an internet user base of about 354 million being third largest user base in world. Source – http://articles.economictimes.indiatimes.com/2015-09-03/news/66178659_1_user-base-iamai-internet-and-mobile-association

²Source: http://www.business-standard.com/article/news-cm/e-commerce-industry-likely-to-spend-addl-500-to-1000-mln-usd-on-infrastructure-logistics-warehousing-till-2017-2020-study-114082100578_1.html

Key questions the senior management needs to ask

1

Are we aware of the fraud vulnerabilities/ areas of revenue leakage in our business? Are our existing revenue assurance frameworks robust enough to mitigate these risks?

2

Do we know if counterfeit products are being sold through our marketplace?

3

Do we know if the third parties (vendor/ sellers) in our business ecosystem have an adverse reputation among their peers or the public?

4

Is our organisation complying with the statutory requirements such as the Companies Act 2013, Prevention of Corruption Act, 1988 etc.? If not, can the non-compliance impact our future funding prospects?

5

Have we gauged the effectiveness of our existing fraud risk management framework?



Our solutions

While most e-commerce organisations have realised the need for a strong internal team to manage fraud-risk-related vulnerabilities, working alongside third-party forensic experts can reveal inadequacies in the prevailing fraud risk management framework, as well as make organisations aware of newer fraud schemes.

Deloitte has been recognised as the world leader in forensic and dispute services by Kennedy Research 2014 , and our India practice has a dedicated e-commerce-focused team offering select services to companies. Some of these services are listed below.

Revenue leakage and fraud risk management (RLFRM)

We can assist your organisation in:

- Assessing different revenue generation avenues and the associated processes
- Assessing processes pertaining to customer-wallet management
- Conducting maturity assessment of the current state of revenue assurance and fraud management practice both at marketplace and digital wallets
- Conducting gap assessment by identifying potential areas of revenue leakages or frauds that are unaddressed in the existing revenue assurance processes
- Formulating and implementing customised RLFRM framework (including dashboard) to mitigate revenue leakages and potential fraud areas
- Operationalising RLFRM function through managed services support

Brand protection advisory

We can assist in assessing your organisation's current brand perception among stake holders such as customers and partners through:

- Analysis of internal information such as QRC (Query, Resolution and Complaint) data base, billing, provisioning, wallet transactions and customer satisfaction score to arrive at brand impact indicators
- Mystery shopping throughout the customer life cycle (onboarding experience to off-platform shopping experience) to determine the customer experience as well as flag the potential fraud risk areas (e.g. counterfeit products), including discreet enquiries to track down the counterfeit goods manufacturers to cut off the product source
- Workshops with key stakeholders to understand key concerns and root cause of issues
- Market/business intelligence across service operations, including vendors, to check for the presence of any counterfeit activity
- Sentiment analysis from social networking properties around customer dissatisfaction, fraud/ misconduct and any other negative brand publicity

Compliance review of third-party sellers

To ensure that sellers adhere to the norms and guidelines prescribed by your organisation, we can conduct onsite checks as well as online website sweeps to ascertain compliance levels. We can:

- Conduct physical checks on the sellers' businesses
- Conduct a visual check at the seller premises as well as the third-party delivery hubs based on compliance requirements to test the product quality, packaging material and product labelling, and packaging dimensions
- Verify the parity between product data (pertaining to quality, certifications etc.) entered into the system and the items actually sold
- Evaluate whether the seller is compliant based on the documents approved by the client

Our solutions Continued...

Cyber forensic incident response

We can help your organisation:

- To be aware of threat profiles and vulnerabilities and to respond effectively, should an attack happen
- Identify potential internal and external threats like customer information scrapping, business logic abuse, malicious attack footprint, etc. through our cyber forensic approach, which blends network forensics, security perimeter forensic analysis, activity forensic and data integrity forensic
- Analyse malware presence through a root-cause-oriented approach using our malware exploration framework, which focuses on reverse engineering the malware to provide insight into micro-grained code and hacked application modules, and on further testing of decoded malwares in an automated environment across all operating systems and digital devices

Competition law

Our competition law experts can help:

- Conduct competition-compliance programmes with data analytics, e-discovery and review of agreements to assess potential anti-competitive behaviour
- Define the relevant market for these businesses through consumer survey and economic and econometric analyses
- Conduct market studies to identify potential scenarios of dominance by looking at aspects such as:
 - Relevant market and defining the product (online and offline retail) and geographic markets using economic theory for the entity under examination
 - Cost structure and the pricing of the product
 - Quantifying whether the player was a dominant player in the “relevant market” by using concentration ratios and indexes
 - Use of sophisticated economic analysis tools like the recoupment test

Fraud risk management

We can help organisations set up a fraud risk management structure including:

- Development of fraud risk mitigation policy
- Comprehensive evaluation of anti-fraud programmes and controls as well as ethics and compliance programme
- Employee fraud awareness training(s)
- Establishment of a whistleblowing hotline
- Development of a Fraud Response Management Plan

Fraud investigation

We can help organisations investigate red flags from whistle-blower hotlines and internal audit reviews through computer forensic and accounting expertise, document and transactions analysis, combined with witness and third-party evidences.

Key Contacts

Rohit Mahajan

APAC Leader and Partner

Forensic- Financial Advisory

Tel: +91 22 6185 5180

Email: rmahajan@deloitte.com

Amit Bansal

Partner

Forensic- Financial Advisory

Tel: +91 22 6185 6764

Email: amitbansal@deloitte.com

Sumit Makhija

Partner

Forensic- Financial Advisory

Tel: +91 124 679 2016

Email: sumitmakhija@deloitte.com

Nikhil Bedi

Partner

Forensic- Financial Advisory

Tel: +91 22 6185 5130

Email: nikhilbedi@deloitte.com

KV Karthik

Partner

Forensic- Financial Advisory

Tel: +91 22 6185 5212

Email: kvkarthik@deloitte.com

Jayant Saran

Partner

Forensic- Financial Advisory

Tel: +91 124 679 3607

Email: jsaran@deloitte.com

Rajat Vig

Partner

Forensic- Financial Advisory

Tel: +91 124 679 2905

Email: rajatvig@deloitte.com

Rohit Goel

Director

Forensic- Financial Advisory

Tel: +91 124-6792340

Email: rogoel@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP).

This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2016 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339), a private company limited by shares, was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458) with effect from October 1, 2015