KPMG

COVID-19: Fraud trends in the e-commerce sector

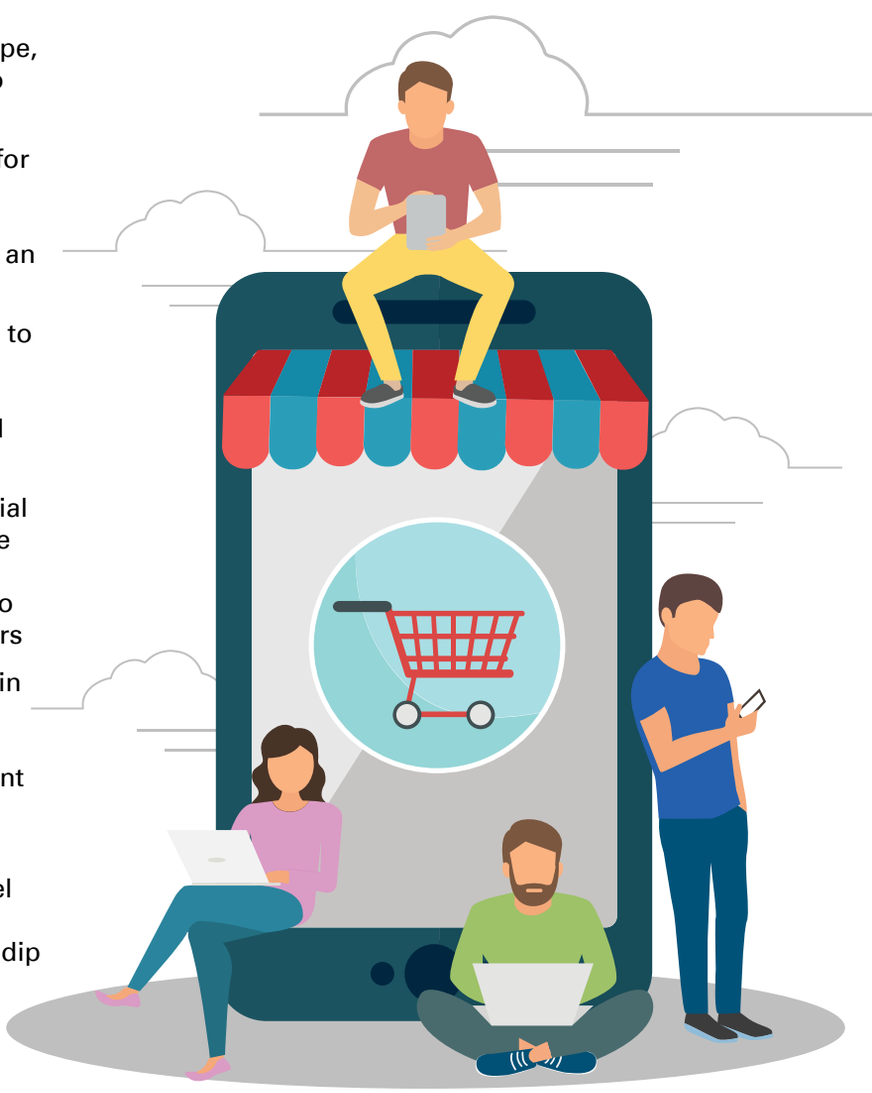
home.kpmg/in

The COVID-19 pandemic has taken the world by surprise as it continues to spread across the globe. The outbreak has triggered an unanticipated health and economic crisis in a short span of time. The pandemic has resulted in the cessation of world trade and has forced human life under quarantine conditions, which could, perhaps, alter the business landscape irrevocably.

With the lockdown being imposed, brick-and-mortar retail operations have been significantly disrupted and consumers are transitioning into digital realms to meet their requirements. The e-commerce sector has witnessed a temporary suspension in the sale of non-essential products and the focus has shifted towards essential commodities that are necessary for survival. The e-learning and entertainment domains have also been beneficiaries of the lockdown since people are confined to their homes. Some consumers have experienced their first online purchase, while others have deepened their online spends. This dynamic change in buying behaviour calls for e-commerce players to reimagine their business and adapt quickly in order to be resilient and respond in a manner that benefits them. Organisations operating under a traditional trade model may need to venture into the e-commerce space to sustain themselves under the evolving business landscape, where consumer buying preferences are likely to change.

As the impact of COVID-19 is expected to linger for the foreseeable future, organisations in the e-commerce sector would need to consider the following direct implications while preparing for an eventful, bigger and faster phase of growth.

- Disruption in the supply chain network owing to the various restrictions on domestic transportation and imports, especially on products from China and other vastly affected geographies
- The unforeseen increase in demand of essential commodities might not be reciprocated by the last-mile connectivity system, including transportation and delivery partners leading to challenges in delivering products to consumers
- In the process of absorbing the sudden spike in demand of essential products, organisations may incur higher costs or lower quality standards and lack implementation of sufficient controls to enable a smooth transition
- Significant cash flow issues for e-commerce organisations in the businesses of travel, hotel booking, movie/event ticketing and cab aggregators, among others, due to an abrupt dip in demand
- Temporary cessation of investments and fund infusion may lead to financial challenges and could also raise business continuity issues for certain players in this sector
- Surge in terms of subscriptions and registrations on organisations' e-commerce portals in the business of supplying essential products and for online subscription-based entertainment
- Likely transition of consumer preference towards online purchase of even non-essential products, post the lockdown period, could result in penetration of e-commerce players in areas that were traditionally dominated by brick-and-mortar stores
- Digital payments will be on the rise as consumers are keen to preserve cash and many e-commerce platforms have temporarily stopped cash-on-delivery options to make payments for online purchases.



Considering the above factors, there could be significant implications for the e-commerce sector due to the COVID-19 pandemic, which may lead to an increase in the possibility of frauds and wrongdoings. This is because fraudsters generally tend to take undue advantage of such situations to defraud susceptible organisations and consumers.

The weaknesses in systems could be exposed and those with nefarious intent will seize the opportunity to exploit the panic, fear and suffering that accompanies a pandemic. The typical frauds and wrongdoings that could take place in this sector in our view are as follows.

A Sales and distribution

- Creation of fictitious customers to misuse sales promotion schemes and cashback offers by employees and fraudsters in collusion with each other
- Undue advantage of special discount schemes meant for consumers as a result of collusion between employees and fraudsters (sellers). In such instances, fraudsters may purchase the products with special discounts through multiple fraudulent consumer accounts and then sell these products once again at higher rates in the open market
- Abuse of new user promotions by consumers by generating fictitious email addresses for wrongfully availing of the discounts/schemes available only for new registered users
- Misuse of the balance amount remaining in electronic gift vouchers that were not redeemed completely by the consumers
- Manipulation of sales/financial data to wrongly indicate eligibility for various incentive schemes applicable for sales personnel/sellers
- Inflated invoices submitted by marketing agencies for various marketing activities on the websites of the marketplaces in collusion with employees of the marketplace.

B Logistics and inventory management

- Pilferage of original products by delivery personnel and delivery of fake products to customers leading to refund/replacement claims on organisations
- Fraudulent refund/replacement claims made by unethical customers, return of fake products in replacement of original products delivered to customers or customers wrongfully depicting non-receipt of products, although the products were delivered to them
- Service providers appointed for domestic transportation and warehousing could indulge in unethical practices, which could lead to pilferage/diversion of products for sale in the open market at higher prices
- Theft/diversion of products stored at the warehouse by employees due to less manpower availability at the warehouse during the lockdown period
- Products received as exchange/returns from customers may be sold to scrap vendors at lower than market rates, as a result of collusion between the vendors and employees. These items are used products received from customers in exchange for purchase of new products on e-commerce portals or defective products returned by customers.

C Procurement

- Organisations may need to urgently adopt alternative procurement channels due to restrictions on imports and domestic transportation. This could lead to appointment of unethical vendors supplying at inflated prices or providing sub-standard quality products/services as a result of collusion between employees and these vendors
- Emphasis on maintaining operations and remote-working scenarios could lead to lack of focus on compliance in organisations during the lockdown period, which may result in procurement of excess material/services than the actual requirement.

D Compliance

- Sale of counterfeit products by sellers to the marketplace to meet the increased demand for essential products during the lockdown period. This could result in potential intellectual property claims against the marketplace for the sale of counterfeit products
- Due to increased demand of essential products, damaged and expired products could be potentially put in circulation in the marketplace by tampering the date of manufacture and/or changing the packing of the products
- Sellers and third parties indulging in bribery and corruption activities to ensure smooth operations during the lockdown period, resulting in potential violation of applicable Anti-Bribery and Corruption (ABC) laws and regulations
- Intense pressure on organisations to quickly obtain goods and clear them through the customs process due to demand for essential products. Third parties and employees could indulge in bribery and corruption activities due to the challenges in sustaining business operations, maintaining profitability levels and avoiding termination/lay-offs due to non-performance. These could result in financial penalties and reputational issues for the organisation/marketplace.

E Cyber frauds

- Fictitious online websites/mobile applications, resembling the original marketplace/organisation's website/application, may be created by cyber criminals to induce consumers to subscribe and make payments to avail of discounts/benefits
- Surge in digital payments by consumers may lead to an increase in hacking and phishing attempts to obtain consumer credentials and diversion of payments to fraudulent bank accounts. The modus operandi of cyber criminals has now taken to the abuse of Application Programming Interfaces (API) that are a bridge between payment portals and shopping carts, whereby the Personally Identifiable Information (PII) of customers could be compromised
- Employees working from home are more vulnerable to fraudsters seeking confidential information due to use of personal devices, unsecured networks and personal (unencrypted) email accounts. These data breaches may lead to financial and reputational losses to organisations.

F Recruitment frauds

- Increase in unemployment and desperation to obtain jobs may lead to submission of fictitious personal and educational qualification documents by candidates hired by marketplaces or organisations to sustain their shortage of manpower due to increased demand. This may lead to hiring of incompetent employees or employees with prior involvement in frauds or wrongdoings.

How could KPMG in India help?

A. Root cause investigation and impact assessment

Remotely deploy specialists equipped with sector and domain knowledge to conduct a detailed investigation into indications/complaints/suspicions pertaining to potential wrongdoings. This activity could enable the management of organisations/marketplaces to take timely corrective action and prevent any possible financial and reputational loss.

B. ABC diagnostic review

Conduct a diagnostic risk review to check adherence to the defined ABC framework. Additionally, during the review, identify transactions, if any, incurred by the organisation, marketplace or third parties associated with the organisation or marketplace in contravention of the ABC laws and regulations.

C. Root cause investigation of cyber incidents

Assist in responding to cyberattacks by undertaking a detailed investigation to identify the root cause, containment of threats, persons involved and recommend steps to secure the environment for preventing further attacks.

D. Fraud risk assessment

Proactive assessment of key business processes to highlight major fraud vulnerabilities and recommend mitigating steps. Fraud risk assessment can help the management to ascertain the effectiveness of the designed processes and controls to reduce the possibility of frauds and wrongdoings.

E. Counterparty due diligence

Services include rapid onboarding checks for new sellers, vendors and third parties; also, provide coverage for refresh checks on existing sellers, vendors and third parties' financial strength, ownership structure, key personnel, litigations, market reputation, regulatory non-compliance, adverse media, willful defaults, among others.

F. Employee background checks

Screening of prospective employees across all levels in a flexible, timely and cost-effective manner through various categories of checks to suit the compliance needs of organisations. The screening process shall include validation of key credentials of a candidate for employment, such as academic qualification, previous employment records, reference checks, criminal and litigation records, adverse web and media records, credit checks, global sanctions and regulatory database checks and substance abuse screening.

G. Awareness sessions

Undertake remote awareness sessions for employees on fraud prevention and detection, prevention of cyberattacks, bribery and corruption risks and the importance of compliance with ABC laws and regulations among others.

KPMG in India contacts:

Vijay Chawla - Banglore
Partner and Head
Risk Advisory
T: +91 80 6833 5509
E: vschawla@kpmg.com

Jagvinder S. Brar - Gurugram
Partner and Head
Forensic Services
T: +91 124 336 9469
E: jsbrar@kpmg.com

Harsha Razdan - Mumbai
Partner and Head
Consumer Markets and Internet Business
T: +91 22 6134 9663
E: harsharazdan@kpmg.com

Mustafa Surka - Mumbai
Partner
Forensic Services
T: +91 22 6134 9313
E: mustafasurka@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia