KPMG

COVID-19: Evolving frauds in Consumer Markets sector

home.kpmg/in

In an unprecedented chain of events, the outbreak of COVID-19 has amplified the prevailing slowdown in the global economy, as well as in the Indian economy. The nationwide lockdown is likely to have a colossal impact on the economic situation. The preferences of the customers have also shifted as they are exercising caution about where, what and how they make their purchases.

We still know little about the COVID-19 virus and its long-term implications. It has potentially led to multiple scenarios as follows, which could lead to significant impact on organisations in the consumer market sector:

- Steep increase in demand of essential products due to panic shopping leading to perceived shortage of products of daily consumption
- Augmented demand for delivery through e-commerce channels and corresponding rise in digital payments, especially for essential products, due to social distancing obligations
- Less demand for non-essential products leading to operational disruptions and consequent adverse impact on their profitability and cash flows
- Retail outlets, except grocery stores and pharmacies, have shut their doors. Retailers, particularly those with physical footprints, are rethinking their current cash positions and trying to assess how they will continue to pay the bills, should the downturn in demand continue for a prolonged period
- Disruptions in raw material supplies due to closure of factories and import restrictions leading to adoption of alternative procurement channels, which are likely to be costlier and/or materials are likely to have quality issues
- Likely job losses and salary cuts, leading to lower consumer spending.

Considering the resultant adverse impact, there is an increased risk and possibility of wrongdoings occurring in organisations operating in the consumer market sector. The typical wrongdoings that could potentially take place in this sector in our view are as follows:

Sales and distribution

- Diversion of products required to be sold in one channel to another channel to claim undue benefits of price arbitrage between the two channels
- Fictitious sales recorded under a program to claim higher benefits in the said program
- Fictitious sales recorded to claim benefits of volume/slab discounts, which are not actually operated in the supply chain.

Sale of damaged and expired products

- Due to increased demand of essential products, damaged and expired products could be potentially put in circulation in the supply chain by tampering the date of manufacture and/or changing the packing of the products.

Artificial inflation of prices

- Hoarding of essential products, which creates superficial scarcity and subsequently, these products could be sold at higher than the stipulated prices.

Counterfeiting

- Due to the perceived difference between demand and supply of essential products, there is a high possibility of counterfeit products being injected in the supply chain. The general public is usually unable to spot differences between genuine and potentially fake products, and thus ends up buying potentially fake products.

Fictitious websites/fake social media accounts

- Fictitious online websites/fake social media accounts could be created to attract consumers to pay upfront for the products. After receiving the payment, fraudsters pocket this money without delivering the products.

Procurement of material and services

- Need to identify alternate procurement channels due to restrictions on imports and domestic transportation. This in turn could increase the risk of collusion between vendors and employees, due to less focus on compliance and urgency of requirement, which could potentially lead to supply of sub-standard quality material/services by vendors at higher prices.

Unauthorised transactions and alterations in the accounting system

- Due to remote working and operational pressures, unauthorised alterations could be made to master databases in the accounting system to make fictitious payments and siphon the funds.

Bribery and corruption

- Irregular payments and/or products (free of cost) could be provided by third parties like transporters/channel partners to statutory authorities, to ensure smooth clearance and transition of goods during the lockdown period. This could lead to potential violation of the applicable Anti-Bribery and Corruption ('ABC') laws and regulations.

Non-compliance of laws and tax regulations

- Shortage of man-power and remote working could lead to non-compliance of certain laws and tax regulations, such as Food Safety and Standards Authority of India ('FSSAI') requirements, Goods and Service Tax ('GST') Act, among others. Also, non-compliance of the laws by third parties/channel partners working with the organisation could expose the organisation to risk of non-compliance.

Disputes

- Disputes related to lease rent payments by commercial establishments for their stores located in malls, multiplexes, amusement parks, among others, could arise on account of lockdown and closure of the commercial establishments
- Disputes with channel partners and retailers on account of additional cost of operation could arise due to lockdown and non-payment of subsidies, fixed monthly payments for window or sign board space, advertisement charges on websites, among others
- Disputes with service providers due to failure of compliance with minimum commitments in terms of volumes, number of people to be employed, among others could arise due to lockdown.

Cyber frauds

- The increase in remote working and multiple internal updates/seeking of information by organisations could lead to avenues for fraudsters to target organisations and their employees to handover their credentials and get unregulated access to the business accounts and network of the organisation
- As organisations have stipulated 'work from home', a spike in ransomware attacks could be possible, where the servers, remote computers could be attacked and encrypted for ransom, bringing the organisation to a complete standstill position
- Use of personal devices, unsecured networks and personal (unencrypted) email accounts, are more prone to data breaches and cyber frauds.

How could KPMG in India help?

Root cause investigation and impact assessment

Remotely deploy specialists equipped with sector and domain knowledge to conduct a detailed investigation into any indications/complaints/suspicions pertaining to potential wrongdoings. Our customised approach would be focused on delivering high-quality outcome within the shortest possible time. This activity could enable the management of organisations to take timely corrective action and prevent any possible financial and reputational loss.

Pro-active data analytics

Pro-active monitoring of data and use of forensic data analytics tools developed for specific areas, such as procurement, payroll, sales and distribution spends among others, could help identify red flags of any existing/potential wrongdoings. KPMG in India has the capability to develop a customised offering with inhouse tools and technology to perform the required data analytics.

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 organization or third parties associated with the organization, during the lockdown period in contravention of the ABC laws and regulations.

Cybersecurity

Assist in responding to cyber threats effectively and efficiently with our bouquet of services ranging from rapid cyber incident response, containment of threats, continuous monitoring to training and capacity building, and take measures to prevent such incidents in the future.

Dispute advisory services

Assist in resolution of commercial and contract disputes. We could support your legal team by dissecting complex issues and providing robust, compelling arguments on financial, commercial, valuation and accounting aspects.

Awareness sessions

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

KPMG in India contacts:

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

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

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

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

home.kpmg/in

Follow us on:
home.kpmg/in/socialmedia

#KPMG josh