Retail sector fraud diagnostics

home.kpmg/in

The focal point…

Retail sector primarily comprises of businesses that sell goods through large stores to the general public. Some typical features of a retail operation are given below:

- Sourcing of products through owned manufacturing facilities, other large scale manufacturers, small scale enterprises and local vendors.
- Inbound transportation of sourced products to either a central warehouse or a depot for onward distribution.
- Outbound transportation to either owned stores or franchise operations for sale.
- Sale of products either through owned stores or franchise outlets or online e-commerce platforms.

Our focus is to help retail companies identify and address the fraud risks arising from vulnerabilities in their operations.

Key vulnerabilities you should watch out for

Supply chain frauds

Procurement

- Procuring material or services either not required or procuring more than the required quantity
- Paying more than the market price
- Transactions with non-existent vendors
- Conflict of interest scenarios with vendors and kickbacks for procurement received by company employees.

Inbound

- Short receipts of material in collusion with vendors or transporters but payment made for the full quantity as per the invoice
- Deliberately accepting substandard/expired/short life goods
- Theft/pilferage of goods in transit and diversion of goods for sale in the grey market.

Outbound

- Forging of documents required to take loaded vehicles out of warehouse premises
- Seal manipulation and stealing/changing goods in transit and consequent short deliveries to stores
- Planned robberies and vehicle hi-jacking especially for those containing high-value materials.
- Pilferage of original products by delivery personnel and delivery of counterfeit products to customers.
- Fraudulent refund / replacement claims made by customers for return of counterfeit products in replacement of original products delivered to them
- Pilferage of cash collected from cash-on-delivery customers by delivery personnel.

Frontend frauds

Sales

- Payment in fake currency
- Credit/debit card frauds
- Misuse of credit notes
- Misuse of cash refunds/item returns
- Price manipulation/markdowns
- Sale on manual bill books
- Pilferage of inventory by manipulation of the barcode / Point of sales system (POS).

Store inventory

- Misuse of items that ideally should be disposed of (for instance after/nearing the expiry of their shelf life)
- Misuse/losses in home deliveries
- Theft of inventory in collusion with stores/outlet employees
- Deliberate product sabotage resulting in the loss of market reputation / brand image of the organisation
- Expired products sold to scrap dealers who sell these products at price lower than that of the organisation.
- Sale of counterfeit products by sellers in retail stores or online marketplaces / portals, resulting in potential violation of contractual terms by sellers.

Promotions

- Misuse of promotions/marketing schemes/loyalty programmes.
- Misuse of gift vouchers/gift cards.

Other areas

Confidential data

Theft of confidential information including:

- Customer data (including online transaction details)
- Product master data
- Suppler information
- Product Intellectual Property (IP)

The above can be sold by perpetrators to competition.

Bribery and corruption

- Making improper payments either directly or indirectly to authorities in relation to licenses, permits or taxation
- Real estate acquisition frauds with kickbacks to employees/government authorities.

How we can help you

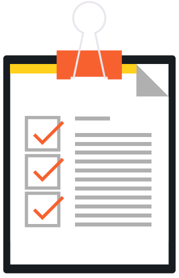
Our approach for conducting a fraud risk diagnostics for a retail operation is detailed below:

Understanding the process

- Obtain an understanding and broad overview of the existing processes, systems, controls and documentation maintained for procurement, sales, inventory management.
- Obtain an understanding of the information system to monitor the operations at the company's own stores and/or franchisees.
- Understand the roles and responsibilities of the persons involved in the key processes for daily operations.

Analysing the data

- Identify the sources for Point of Sales (PoS) data available.
- Extract required data from identified sources and perform data analysis including but not limited to:
  - sales pattern for customers
  - discounting/credit note usage
  - price variations/adjustments
  - manual billing
  - PoS user analysis
  - invoice wise/product wise analysis
  - invoice cancellations/refunds
  - promotion codes/coupons
  - collections on sales and cash deposits.
- Extract the required accounting transaction data including but not limited to:
  - procurement
  - marketing expenses
  - vendor ledgers
  - inventory (adjustments for damage/non-moving/take backs)
  - logistics (inbound/outbound).
- Perform a detailed analysis on the above extracted data and identify sample transactions for detailed review.



Testing documentation and gathering market information

- Based on the red flags identified from data analysis performed, undertake document review on a sample basis to verify supporting documentation including but not limited to:
  - vendor quotations
  - vendor selection documents
  - vendor invoices
  - delivery/dispatch documents
  - sales invoices
  - order documents
  - credit notes
  - inventory records
  - cash deposit slips
- Attempt to gather discreet market intelligence of the company employees, vendors and third parties interacting with the company, as considered necessary.

Analysing the gaps and making recommendations

- Based on the red flags identified from data analysis and document review identify gaps attributable to:
  - Process
  - System
  - People
- For the gaps identified, suggest practical recommendations to mitigate fraud risks.

While this is the broad outline of our approach, it is highly customisable, and can be modified to suit the specific requirements of the client.

Potential benefits

- Fraud risks specific to retail operations are identified and mitigated by implementing practical recommendations that help address these risks.
- Identify and fix loopholes if any in systems and processes in place which may be misused by the owned store or franchise store operators for undue benefits.

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
Forensic Services
T: +91 124 336 9469
E: jsbrar@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.