KPMG

Sales and distribution spends vulnerability assessment

home.kpmg/in

The focal point…

All modern day organisations have set-up a vast network of distributors to help cater to its customers. Some typical features of such a network include the following:

- Supply to outlets across geographies
- Low credit risk for companies with credit risk being passed on to the distributors
- Trade schemes, discounts, rebates and incentive models to drive high volume sales
- Operations decentralized and managed by regional or branch offices of companies
- The network of distributors operate on a uniform distribution management software.

This network of distribution requires constant support of marketing and sales initiatives to sustain the growth plans of any company. The 'high rewards' offered to sustain growth often come with 'high risks', which need to be monitored on an ongoing basis.

Our focus is to help companies identify and address the fraud risks arising from vulnerabilities in their sales and distribution spends process.

Key vulnerabilities you should watch out for

Sales promotion or Below The Line (BTL) spends

Secondary sales

- Creation and maintenance of fictitious retailers / dealers in order to show a wider reach by channel partners and sales field force
- Recording of secondary sales during specific period of sales cycle
- Manipulation of secondary sales in system to claim undue benefits of trade schemes
- Channel-stuffing towards the end of the sale cycle in order to obtain undue benefits of channel program / loyalty program eligible for retailers / dealers.

Distribution of scheme benefits

- Recording of fictitious sales in DMS in order to obtain undue scheme benefits by the channel partners
- Miscommunication of schemes and manipulation of sales / discounts / schemes which led to benefits either not been passed or partly passed to the eligible recipients by the channel partners
- Submission of falsified documents / acknowledgements as an evidence for distribution of scheme benefits that were not passed to the eligible recipients by the channel partners
- Creation of fictitious vendors / customers on online marketplaces / portals to misuse sales promotion schemes, discounts and cashback offers.
- White goods to be distributed as a part of the secondary sales scheme were either not purchased or purchased from related vendors at an inflated value by the channel partners / sales field force.
- Preferential pricing offered to select customers on online marketplaces / portals in collusion with employees
- Misuse of the amount remaining in the electronic gift vouchers by employees, which were not redeemed completely by the customers.

Procurement of gift for schemes

- Unauthorised distribution of gifts amongst employees due to excess quantity purchased
- Fictitious invoices submitted with claims for purchase of gifts
- Kickbacks received by employees for procurement of gifts from related / connected parties at higher price.

Return on investment subsidies to distributors

- Manipulation of financials by channel partners and sales team to demonstrate their eligibility for subsidies and obtain undue benefit of subsidies from the organisation
- Alteration of actual sales data to demonstrate eligibility for subsidies.

Slow moving / expired stock

- Slow-moving inventories classified as damaged goods by the channel partners in order to avail undue benefits by transferring such slow moving inventories back to the organisation instead of pushing the same in the market
- Slow moving or aged stock sold in grey market at lower price, jeopardising brand and organisation reputation
- Expired inventories not destructed and tampered to change the manufacturing date. Sale of these inventories as fresh inventories in tier-2 and tier-3 cities jeopardising the reputation of the organisation and also impacting its sales
- Inventories meant for sale through one channel, diverted and sold, to another channel / exported outside the country due to price arbitrage between the two channels / countries

Incentive to sales force

- Manipulation of sales target to demonstrate achievement by the sales force
- Alteration of actual sales data / price data to demonstrate achievement of eligibility criteria for earning sales incentives.

© 2020 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Marketing events and campaigns (including visibility schemes)

- Fraudulent invoices processed for marketing events and advertisements campaigns, without the events being conducted and airing of commercials. Fictitious or morphed supporting documents submitted to indicate that the said activities were conducted
- Morphed or fictitious photographs submitted with multiple claims by channel partners to reflect existence of outlets / signboards to indicate that the said window space was provided by the outlets or signboard was installed at the said outlets
- Theft of sensitive information related to the innovation and research or marketing plans of the organisation.

Front end sales Frauds

- Mis-utilisation of the Point Of Sale Material ('POSM') provided by organisations to channel partners POSMs not distributed to the channel partners either sold in market or sold as scrap by the channel partners
- Payment in fake currency or stolen / bogus credit / debit cards
- Payments credited to personal e-wallet account of employees
- Misuse of credit notes and cash refunds / merchandise returns.

How we can help you

Our approach for conducting sales and distribution spends vulnerability assessment is detailed below:

Plan and diagnose

Understanding of processes and systems

- Obtain an understanding of the company's existing processes, systems, controls for sales and distribution initiatives and the relevant supporting documentation required for the same.

Analysis of relevant data

- Design fraud scenarios specific to the company and extract relevant data from systems to perform data analytic routines and identify red flags.
- Analyse the relevant data and study key functionalities of the distribution management system identified based on understanding obtained, in our in-house forensic lab.

Detect

Identification and review of fraud risks

- Based on red flags identified from data analysis, undertake document review on a sample basis.
- Attempt to gather discreet market intelligence of company employees, vendors and third parties, as considered necessary.
- Identify pervasive vulnerability risks prevalent at an industry level and specific to company's business processes.
- Attempt to obtain sample-based telephonic confirmations from recipients regarding the receipt of purported benefits.

Recommend

Way forward

- Based on the red flags identified from data analysis, document review and database testing 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

- Conducting scenario based testing can help to ensure focus on fraud risks relevant and applicable to the company's operations.
- Identifying fraud risks in marketing and promotional initiatives undertaken by the company as part of their sales and distribution spends.
- Identifying loop holes (if any) in the distribution management system of the company that can be misused by the distributors for undue benefits.
- Implementing practical recommendations to mitigate fraud risk arising from gaps noted in the process and system involved in the sales and distribution spend life cycle.

© 2020 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

KPMG in India contacts

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader – Global Cybersecurity
T: +91 124 336 9400
E: atuteja@Kpmg.com

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

Maneesha Garg
Partner and Co-Head
Forensic Services
T: +91 120 386 8501
E: maneesha@kpmg.com

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

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/social media

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.

© 2020 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This publication is meant for e-communication only.