Sales and distribution spends vulnerability assessment
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
- Fake outlets/dealers created in the distribution software to show wider reach.
- Inflation of sales during specific periods of a sales cycle to earn higher incentives.
- Manipulation of secondary sales/secondary schemes in order to claim undue benefit of trade schemes.
- Irregular pattern of billing to channel programme/loyalty programme outlets during the end of the sales cycle evidencing channel-stuffing.

Distribution of scheme benefits
- Miscommunication or non-communication of scheme benefits to outlets/dealers.
- Scheme benefits are either partly distributed or not distributed to eligible recipients.
- Fraudulent documentation generated to evidence distribution of scheme benefits.

Procurement of gifts for schemes
- Purchase of gifts in excess of the requirement and excess quantity distributed between the distributors and/or company employees.
- The gifts for distribution are either purchased at higher prices or from related parties resulting in conflict of interest situations and kick-backs received by company employees.

The network of distributors operate on a uniform distribution management software.

Marketing events and campaigns
- Inflation of invoices or submission of fake invoices by marketing agencies with/without collusion of company employees.
- Invoices of vendors for marketing activities routed through intermediaries owned directly or indirectly by company employees.

Incentives and subsidies

Return on investment subsidies to distributors
- Manipulation of financial numbers to obtain undue benefit of return on investment subsidies.

Other subsidies to distributors
- Manipulation of vehicle routes and distances travelled to pay higher subsidies to distributors.
- Payment of employee cost reimbursement subsidies to distributors for ghost employees.

Slow moving stocks
- Distributor showing slow moving stocks as damaged goods to get undue benefit from the company.
- Slow moving or aged stock taken back from retail outlets for disposal sold in the grey market at a lower price thus cannibalising the sales of its own products and jeopardising the brand’s reputation.

Incentive to sales force
- Manipulation of sales targets to demonstrate achievement thereof by the sales force.
- Alteration of actual sales data/other data to demonstrate achievement of eligibility criteria for pocketing sales incentives.
How we can help you

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

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.

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.

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.

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.
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.

© 2019 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 document is meant for e-communication only.