Deloitte.

# Decoding Frauds in the Manufacturing sector

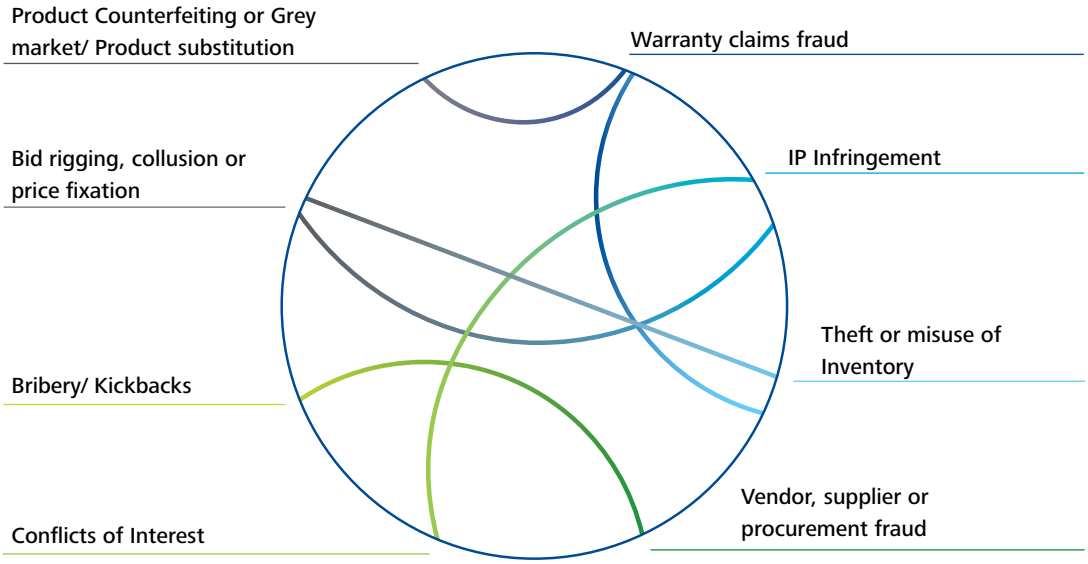

www.deloitte.com/in

India's manufacturing sector is vital for its economic progress. It contributes to approximately 16 percent of the country's GDP and with a potential to grow more, India's attractiveness as a manufacturing centre for foreign companies is all too apparent.

Deloitte's Global Index[1] for 38 nations (2013) ranked India as the fourth most competitive manufacturing nation and is expected to be ranked as the second most competitive manufacturing nation, next only to China in the next five years. It thereby gives domestic entrepreneurs and international players numerous opportunities to invest and grow in the segment. However, with global fraud reports[2] estimating the median loss in the manufacturing sector at USD 250,000; effects arising from such incidents of fraud and/or misconduct can thus have an adverse impact on this growth.

The manufacturing sector is often one of the most vulnerable sectors, which is exposed to the risk of fraud and corruption. Some of the most recent frauds in the manufacturing sector that have caused significant losses to companies have been due to inferior product quality triggering product recalls, warranty claims fraud and IP infringement. In some cases, these have also resulted in criminal/ civil actions due to regulatory and statutory violations. Additionally, in our experience, one of the other most common frauds in this sector is inventory frauds, related to the theft or misuse of stocks, which continues to be a cause of concern.

**Key vulnerabilities and fraud risks in the Manufacturing sector**




1 Source: Deloitte's Global CEO Survey: 2013 Country manufacturing competitiveness index ratings

2 Source: ACFE 2014 Global Fraud Study

# Overview of some fraud risks

In the recent past, Manufacturing companies have been daunted by some of the frauds listed below:

## Product Quality Frauds

Frauds owing to inferior product quality usually involves the use of substandard materials in production or in the assembly line for manufacturing of finished products. These can also include fudging of records to meet certain tests or regulatory requirements (like emission norms), purchasing poor quality materials from vendors who pose to be potential conflicts of interest. Some of these vendors might also be returning undue favors or a kickback for inferior quality material. Additionally, there are cases where a manufacturer's internal quality control may not be able to detect poor quality material as control procedures can pick defects only after the complete manufacturing process is over. As margins get squeezed, manufacturers tend to sub-contract critical and non-critical production processes to third parties. If sub-contractors are used without proper due diligence, manufacturers tend to become vulnerable to issues related to product counterfeiting or substitution. Therefore, implementing proactive measures within an anti-counterfeiting program, which includes conducting third party due diligence and performing a fraud risk assessment at the procurement, manufacturing and supply-chain processes level, can help identify leakages, if any, and significantly help deter counterfeiting or substitution.

## Warranty Claims Fraud

Warranty claims amount to huge costs for manufacturing companies and can have a direct impact on product quality and customer satisfaction. It has become quite simple to circumvent whether a product is filed for a basic product warranty or extended warranty period. Hence, being able to identify questionable or suspicious patterns of warranty claims is gradually becoming the focus. This can be done by analyzing the warranty claims using forensic data analytics tools. Such an analysis can also help provide early warning signs on any quality issues and focus on the main problem areas.

Counterfeit products also find their way into warranty claims. These are filed by service providers through the use of genuine serial numbers on counterfeit units/ parts. This is done with the intention of defrauding the manufacturing company and thus stealing genuine or refurbished parts by making false warranty claims. By performing a proactive forensic data analytics exercise on warranty claims filed by customers, fraudulent claims (if any) can be identified and eventually significant amounts of fraud loss can be prevented in the future.

## IP Infringement

Intellectual Property has now become highly important and valuable, while also becoming more difficult to protect over a period of time. The theft of Intellectual Property such as trade secrets, patents, drawings & designs, trade mark or technology are quite common in the manufacturing sector. This infringement of patent/ intellectual property rights can result in the company's products finding their way into the counterfeit/grey market. This can not only cause substantial damage to the sales and revenue but also lower customers' confidence and the manufacturer's reputation. Therefore, conducting third party and senior management integrity due diligence should be the first key step to address this issue.

## Inventory Frauds

Inventory frauds usually involve the theft of goods or materials from a company. The perpetrator may try to cover up the theft by falsifying computer records related to quantities in-hand or may knowingly allow losses to occur (in the case of a collusion). Some preventive measures that can help detect inventory frauds are regular counting cycles, organized warehouses, strong inventory record-keeping along with good picking/ packing/ receiving and stocking procedures supported with related technologies (such as bar code scanning, radio frequency identification and GPS tracking for stocks in-transit).

# Decoding frauds to improve product quality and prevent loss

The success of a fraud prevention program can increase if people feel that their wrongdoing can be detected. However, this success also depends upon the actual mechanisms implemented and their ability to detect frauds.

Manufacturing companies should have a robust fraud risk management framework. The framework should ideally continuously improve the fraud risk management strategy while regularly measuring the current and desired state of the business, in terms of, effectively preventing, detecting and deterring fraud utilizing the techniques of fraud risk management and forensic data analytics. At Deloitte, we call this approach as the Diagnose, Detect and Respond strategy.

By conducting a periodic fraud risk assessment and identifying the specific fraud schemes that can pose the greatest threat to the business (particularly in the areas vulnerable to frauds, as mentioned above), we can help categorize those areas that merit additional investment in targeted anti-fraud controls. With more than half of the organizations[3] unable to recover their losses, proactive measures to prevent fraud thus become critical. Management should continually assess the organization's specific fraud risks and evaluate its fraud prevention programs in light of those risks.

Companies can also prevent fraud losses by proactively using forensic data analytics to detect, prevent and control fraud and corruption issues. This can be done by performing tests on a periodic basis on high risk transactions or areas of business that can identify and isolate suspicious financial transactions within the vast data fields that hum away in the course of everyday business. This in turn, for example, can help manufacturers to identify areas for improvement in product quality and/ or yield substantial warranty cost reductions. Therefore, manufacturing companies need to proactively carry out periodic analysis of relevant data to stop fraud, identify emerging issues related to product quality as well as get to the root-cause faster.

A timely detection of fraud incidents can go a long way in containing the loss and improving the chances of recovering any loss an organization may suffer due to fraud. It is time for organizations to ensure that their current fraud risk management strategies are revised to be in line with current fraud trends and adequate enough to take care of future growth. In addition, increasing ways of preventing and detecting frauds proactively by using forensic data analytics and performing third party due diligence that include background checks of individuals and/or entities can help organizations to mitigate fraud risks.

3 Source: ACFE 2014 Global Fraud Study

# How can Deloitte help

If you suspect that a fraud has occurred, don't hesitate to contact us. Fraud detection requires specific investigative protocols be followed and evidence handled carefully so that further loss to the organization can be prevented. In these types of situations, time is of the essence. Your chances of recovering what is lost are maximized by reacting quickly to the situation. Deloitte's Forensic team can help counsel you through this process. We can help you determine if a forensic review of your records is necessary and maximize your recovery, if a fraud did occur.

Some our key Proactive and Reactive Forensic services are provided below:

| Forensic Services | Service Offerings | Approach |
|---|---|---|
| **Antifraud Consulting - Fraud Risk Management** | • Fraud risk assessment<br>• Fraud vulnerability diagnostic that involves identification of fraud risks in key business processes and recommend effective antifraud controls or a risk mitigation plan<br>• Fraud awareness training<br>• Whistle blowing hotline services | Primarily Proactive |
| **Forensic Data Analytics** | • Analysis of material classes of financial transactions<br>• Analysis of billing data of vendors and sales invoices of customers<br>• Identifying unusual relationships in non-financial data – using demographic details of employees, customers, vendors, attendance records etc.<br>• Analysis of systems logs | Proactive + Reactive |
| **Business Intelligence Services** | • Background check of key personnel and business partners, such as, vendors, suppliers, contractors, etc. | Proactive + Reactive |
| **Computer Forensics** | • Forensic imaging of electronic devices for analysis to find evidence (E.g. email searches and disk imaging)<br>• Discover system logs and unauthorized access to secured areas<br>• Security testing of IT infrastructure (E.g. trail of enabling and disabling portable drives, virus threats, etc.) | Primarily Reactive |

# Contact us

**Rohit Mahajan**
Senior Director and Head of Forensic services
Deloitte Touche Tohmatsu India Private Limited
T: +91 22 6185 5180
E: rmahajan@deloitte.com

**Amit Bansal**
Senior Director, Forensic services
Deloitte Touche Tohmatsu India Private Limited
T: +91 22 6185 6764
E: amitbansal@deloitte.com

**Veena Sharma**
Director, Forensic services
Deloitte Touche Tohmatsu India Private Limited
T: +91 22 6185 5213
E: vesharma@deloitte.com