KPMG

Supply chain fraud

A holistic approach to prevention, detection, and response

kpmg.com/us/forensic

Supply chain fraud is a widespread and increasing global business risk for organizations. According to the Association of Certified Fraud Examiners (ACFE), 83.5 percent of fraud cases it surveyed in 2016 featured asset misappropriation schemes, which include fraudulent billing and disbursement schemes.[1] In today's global market, collusive kickback arrangements, bribery and corruption, and bid rigging are increasingly common and becoming harder to detect.

Modern supply chains are more vulnerable to fraud due to their global reach, the depth of supplier networks, the sheer number of transactions or volume of financial activity, the increasing resource needs to combat fraud, and the complexity of information technology systems. Every link in a supply chain represents opportunities for fraud or misconduct.

However, many companies do not take supply chain fraud prevention seriously. According to the ACFE, 44.7 percent of the fraud cases it surveyed were discovered through a tip or by accident, while only 39.2 percent of the fraud cases were discovered by Internal Audit, management review, account reconciliations, or document examination.[2]

Companies that do more to protect themselves from supply chain fraud are less likely to suffer the consequences. This paper discusses the scope and impact of supply chain fraud, the areas of vulnerability in the supply chain, and key measures to prevent and detect supply chain fraud.

[1] *Report to the Nations on Occupational Fraud and Abuse,* Association of Certified Fraud Examiners, 2016.

[2] *Report to the Nations on Occupational Fraud and Abuse,* Association of Certified Fraud Examiners, 2016.

The fraud epidemic

Enabled by the increasing complexity of supplier networks, technology, and the global reach of manufacturing operations, supply chain fraud is on the rise. And while frauds within the supply chain can generate significant headlines in news media, most fraud in the supply chain creates a slow drip of losses, comprising non-newsworthy events that can aggregate to large losses over time. Organizations that fail to identify areas of vulnerability in their supply chains and enact proper internal controls are at greater risk of fraud or misconduct throughout all points within the supply chain — from the identification of raw materials suppliers to the sale and distribution of finished goods into the market.

Who commits supply chain fraud?

Supply chain fraud can be perpetrated by individual actors or through a collusive arrangement between multiple individuals or organizations. According to KPMG's 2016 survey, "Global Profiles of the Fraudster," 65 percent of the frauds surveyed were enacted by employees of the victim organization; the remaining frauds were perpetrated by parties external to the organization.[3] Employees that commit fraud often have the opportunity to manipulate records or otherwise exert influence on the organization's operations. External parties engaged in fraud against an organization may include former employees, customers, suppliers, or unrelated outsiders who have identified weaknesses in the organization's internal controls.

In instances in which an employee is involved in the fraud, organizations generally experience more significant financial losses. However, hybrid fraud schemes, such as those in which employees collude with competitors or other outside individuals or organizations, may be especially threatening to an organization, as they can be extremely difficult to detect. In general, an organization is at its highest risk of fraud when the three components of the "fraud triangle" come together: the perpetrator can rationalize the fraud, has opportunity to carry it out, and is incentivized to do so.

How are supply chains targeted?

Because of their complexity, supply chain operations provide abundant opportunities for fraud or misconduct, both by employees and external parties. Employees, vendors, regulators, service providers, and others may attempt to identify weaknesses and susceptibility in the supply chain. These weaknesses can occur throughout all stages of the supply chain, from the sourcing of raw materials to the processing of inventory returns. Common supply chain fraud schemes include:

- Kickbacks on raw material purchases
- Foreign Corrupt Practices Act (FCPA) violations
- Intellectual property (IP) theft
- Improper use of production assets
- Counterfeiting and sale of goods on grey markets
- Improper rebates
- Misappropriation of scrap, raw materials, or finished goods
- Fraudulent certificates of origin
- Free trade zone fraud
- Use of conflict minerals
- Office of Foreign Asset Control (OFAC) violations
- Human trafficking and child labor law violations
- Quality assurance fraud
- Disbursement fraud, including billing schemes and check tampering
- Inventory fraud, including purchasing and receiving schemes and false sales.

With seemingly endless possibilities for fraud or misconduct within the supply chain, it is critical for management to understand the impact these types of incidents may have on the organization's strategic goals and financial success and to implement appropriate risk mitigation strategies to help prevent these types of schemes.

[3] "Global Profiles of the Fraudster," KPMG International, May 2016.

In 2007, the U.S. Food and Drug Administration (FDA) identified certain contaminants in pet foods that were imported from China into the United States.[4] In addition to the retail sale of this contaminated pet food, certain portions of this pet food were used to produce animal feed that was fed to hogs and chickens that were ultimately subject to human consumption. The discovery of these contaminants led to a lengthy investigation and the recall of over 150 brands of pet food. The FDA indicted several Chinese and U.S. individuals and companies for their role in the distribution of these products.

In addition to the costs of the product recalls, the damage to brand reputation, and the costs of investigations by the FDA and other regulatory bodies, companies paid out $24 million to consumers and law firms as legal settlements in product liability suits.[5] Recalls of pet food as a result of potential contamination continues today, as the FDA reports frequent voluntary recalls of pet foods by popular brands for the presence of such contaminants as pentobarbital, salmonella, and listeria.[6]

The impact of supply chain fraud

The current regulatory environment, including anti-bribery and corruption provisions, child labor laws, import and export laws, and health and safety regulations, seeks to curb misconduct in the supply chain. However, organizations and their third-party service providers may attempt to circumvent regulations to generate operational efficiencies or cost savings. The discovery of an organization's failure to comply with regulations can have catastrophic effects on the supply chain:

- Manufacturing slowdowns or shutdowns
- Inability to supply customers or increased time to market
- Quality or capacity reductions
- Damage to the brand and increased media/advertising costs
- Loss of market share
- Increased insurance costs
- Product recall costs, including the costs of shipping and destruction of goods
- Investigations or audits by regulators, resulting in increased compliance costs
- Investigations or audits by customers, resulting in chargeback costs
- Litigation costs
- Distributors, wholesalers, or retailers requiring credits.

In addition to the costs of investigations, legal action, and remedial action, instances of fraud in the supply chain can distract management from their key business focus and negatively impact the organization's productivity. Because of this, it is critical for organizations to understand the vulnerability of their supply chains to fraud and misconduct and take appropriate action to prevent and detect this behavior.

[4] FDA website, Animal & Veterinary/Safety & Health/Recalls & Withdrawals Section, "Melamine Pet Food Recall of 2007"

[5] USA Today website, Money Section, "Tainted pet food suit settled for $24 million", Julie Schmit, May 23, 2008

[4] FDA website, Animal & Veterinary/Safety & Health/Recalls & Withdrawals Section

KPMG

Why are supply chains vulnerable to fraud?

Today's supply chains are impacted not only by the volatility of supply and demand but also by local pricing issues, plant capacities, weather/natural disasters, and complex constraints and opportunities in supplier networks. Successful organizations take advantage of these factors to improve their businesses, but with these factors comes the risk of fraud and misconduct. Supply chains are highly vulnerable to fraud due to the complexity of the environment in which they operate and improperly designed systems of internal controls.

As supply chains have evolved and become more complex to meet the needs of global organizations, it has become harder to ensure that critical fraud controls are in place throughout the supply chain. Organizations with complex, multinational supply chains involving a large number of third parties are likely to be subject to more regulatory oversight and have a higher susceptibility to external systemic shocks. In these organizations, the risk of fraud, waste, or abuse in the supply chain is high and can be costly to address. A successful supply chain is one in which an organization has mitigated most of its fraud risk in an economically feasible manner.

Complex supplier networks

Supply chain risks not only extend to the organization's direct suppliers but also to subcontractors who provide source materials or subcomponents to the suppliers. This complex network of suppliers includes not just the various layers of vendors serving suppliers but also the legal, financial, and operational issues inherent in those relationships. Without insight into those subcontractors, organizations may be unaware of weaknesses in the internal control structure, systems of quality control, or sourcing of the materials used by these suppliers.

The monitoring of suppliers and their subcontractors is becoming increasingly complex and challenging due to the insufficiency of available data and the number of resources required to monitor these third parties. While organizations

As organizations enter and operate in new markets, they are likely to rely on third parties, many of whom operate far from headquarters, in a foreign language, with different customs and ways of conducting business. The U.S. FCPA makes it unlawful for certain entities and individuals to make payments to foreign government officials to assist in obtaining or retaining business. The majority of recent enforcement actions under the FCPA have been in relation to acts carried out by agents or intermediaries, which have serious repercussions for the organizations that employ these third parties. According to the U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC), "Risk-based due diligence is particularly important with third parties and will also be considered by DOJ and SEC in assessing the effectiveness of a company's compliance program."[7]

A successful third-party risk management program generally includes the following elements:

- Identifying the universe of third parties and refining the list to in-scope third parties
- Managing the integrity due diligence process and risk assessment
- Conducting the appropriate level of integrity due diligence.

Subjecting third parties to integrity due diligence procedures is a crucial step in mitigating the risk of misconduct within an organization's supply chain network.

[7] *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, Criminal Division of the U.S. Department of Justice and Enforcement Division of the U.S. Securities and Exchange Commission, November 14, 2012.

KPMG

are increasingly implementing risk-based due diligence procedures to assess their suppliers' compliance with bribery and corruption regulations and exposure to money laundering, terrorist financing, conflict minerals, and other risks, undetected supplier integrity issues may reflect poorly on the organization if they become public.

Foreign jurisdictions

The vulnerability of supply chains to fraud and misconduct is further enhanced by the risks inherent in global operations. As organizations expand their supply chains to emerging markets, they face increased exposure to bribery and corruption and to local customs that are not in line with regulations. Further, such behavior is difficult to detect, as it may be costly for an organization to deploy in-country resources, there may be language constraints, or it may be difficult to obtain the data necessary to identify fraudulent behavior.

Because supply chains are global, individuals seeking to commit misconduct within the supply chain often choose to operate in those locales in which they feel safest. Often, these are locales in which controls and/or regulatory oversight are lax. Additionally, organizations that attempt to take legal action against individuals involved in fraud or misconduct in unfamiliar environments may find such litigation difficult or overly costly, thus decreasing the organization's motivation to pursue such matters. The perception that an organization will not seek redress against instances of fraud or misconduct in certain locales may allow the perpetrator to rationalize his or her behavior.

Technology vulnerability

The complexities of the information technology (IT) solutions that organizations require to manage the extended supply chain also increase the potential for fraud. According to KPMG's 2016 survey of 750 fraudsters, technology was a significant enabler for 24 percent of fraudsters.[8] Examples of technologically enabled frauds in the supply chain include fraudulent wire transfer schemes, in which fraudsters subvert the organization's payment controls by using malware or phishing sites to steal bank account log-in information for purposes of transferring money out of the organization.

Adding to the complexity of IT systems is the increasing number of electronic records and systems. Many organizations now have more information than they can effectively manage. This hampers preventative and detective processes and procedures that could be used to detect anomalous transactions, as data analytics must be properly designed to search among large volumes of transactions to identify those displaying red flags. Further, according to "Global Profiles of the Fraudster," proactive data analytics detected only 3 percent of the frauds considered in the survey.

The more complex an organization's IT system, the greater the challenge that the organization faces in properly limiting access and developing a strong IT internal control structure. With the increasing threat of cyber fraud, it is more important than ever that organizations build defenses against hackers and criminal organizations that seek to gain unauthorized access to the organization's IT system. Organizations that lack the skills to appropriately defend against cyber fraud may be unable to stay on top of critical issues in this rapidly changing landscape.

Weaknesses in internal controls

Individuals looking to perpetrate fraud against an organization are increasingly taking advantage of weaknesses in the organization's internal control structure. According to KPMG's 2016 survey, 27 percent of the fraudsters exploited weaknesses in internal controls, up from 18 percent in 2015. Further, 61 percent of the fraudsters benefitted from weaknesses in internal controls that allowed the acts of fraud or misconduct to remain undetected. In a difficult global economic climate, many organizations are cutting costs at the expense of a less robust system of internal controls, allowing for greater exploitation of vulnerabilities by fraudsters.

Properly managing risk within a supply chain is a crucial investment strategy for organizational success. It produces an environment for cost savings, enhances time-to-market, creates greater customer satisfaction, and allows the organization to quickly respond to crises. As with any investment strategy, organizations must perform a cost-benefit analysis to determine the optimal system of preventative and detective fraud controls at a level of affordability that is commensurate with the organization's strategic and operational goals.

In performing a cost-benefit analysis to identify the optimal level of internal controls within the supply chain, it is critical that organizations assign a cost to the potential losses that the organization may face if its system of internal controls is not sufficient to identify acts of fraud or misconduct. As such, organizations should build fraud risk factors into their decision-making models; design key performance indicators (KPIs) that may help to highlight instances of fraud, waste, and abuse; and create models that project likely outcomes of various fraud or misconduct schemes.

[8] "Global Profiles of the Fraudster," KPMG International, May 2016.

How to prevent and detect supply chain fraud

In order to manage the risk of fraud within a supply chain, organizations must put appropriate measures in place to monitor and control the supply chain's operational activities. This requires an integrated and multifaceted approach, which includes elements of prevention, detection, incident response, and program maintenance. These elements include:

- Due diligence on third-party suppliers and vendors
- Hiring the right people and allocating job responsibilities appropriately and with a view to properly managing risk
- Regular risk assessments to identify the current risks and the adequacy of controls
- Employee awareness programs, initiatives, and training
- Detection measures, including continuous auditing and/or monitoring and the use of data analytics
- Incident response plans.

Know your third parties

Organizations should conduct due diligence prior to entering into business relationships with supply chain vendors and other third parties. This due diligence should include obtaining an understanding of the supplier's systems to promote compliance with applicable regulations, legislation, and environmental requirements and adherence to the organization's own standards. In an era of increasing investor sensitivity and consumer expectations with regard to ethical business conduct, organizations should exercise caution when entering into business relationships with suppliers who pose reputational risks to the organization.

Through due diligence, organizations may also identify potential conflicts of interest between a supplier and the organization's own employees. Such undisclosed relationships often allow for collusion or a violation of an otherwise well-written corporate code of conduct.

Establishing the financial stability of suppliers is even more important in the current economic climate. In evaluating a supplier's financial position, organizations should establish that the supplier is financially stable and able to fulfill its contractual commitments. Organizations should also obtain an understanding of the supplier's manufacturing capacity. As supply chains extend and margins are squeezed, suppliers may often use undisclosed subcontractors, which can have serious quality control, safety, environmental, and regulatory implications. Recent manufacturing scandals and mass product recalls demonstrate that organizations assume a large amount of risk when they do not have visibility or control over their full manufacturing process.

Organizations should also establish clear key performance indicators (KPIs) against which vendors, partners, agents, and distributors can be measured, monitored, and audited. These KPIs should include measures of ethical and quality standards, codes of conduct, internal controls, and overall business practices. Organizations should communicate baseline KPIs to their suppliers, along with the consequences for noncompliance, and they may wish to further memorialize these KPIs in supplier contracts or codes of conduct.

Segregate duties

While modern procurement and accounting systems are largely automated, most still rely on the manual input of certain data by employees. This manual activity provides opportunity for employees to commit misconduct, particularly in instances in which the organization has not properly separated roles within its supply chain function. For example, if the organization does not appropriately segregate responsibilities for vendor maintenance, invoice processing, and payment preparation, an employee may be able to divert funds by processing improper payments.

In order to minimize the control each individual has over the supply chain process, no single individual should have the ability to process an entire transaction without the review and oversight of management.

Hire the right people and monitor behaviors

Making informed recruitment decisions, particularly in the case of key positions, can help minimize fraud risk in the supply chain. Employees who are caught committing fraud in the workplace often have a previous history of dishonesty, left previous jobs under a cloud of suspicion, or are in financial trouble. An organization's antifraud program should include a system for identifying these types of red flags. Such systems may include the monitoring of employees' e-mail communications to identify certain trigger words that could be indicative of these behavioral patterns. In such cases in which an organization identifies an employee displaying such a red flag, early intervention and assistance for the employee may alleviate the pressure to commit fraud.

Conduct regular risk assessments

Fraud and corruption risks in the supply chain vary according to industry type, geographical location, transaction volume, and business processes. Conducting regular risk assessments to identify fraud and corruption risks within the supply chain, the likelihood that these behaviors will occur, and the potential consequences make it possible to implement appropriate mitigation strategies and controls.

However, even the most carefully designed and tightly controlled system can be circumvented. Fraud in the procurement process commonly occurs when controls are deliberately overridden by either an individual who knows he or she will not be challenged or by a collusive group of individuals capable of manipulating systems and processes to hide fraudulent activity.

An integral part of the fraud and corruption risk assessment is determining the effectiveness of existing controls, thresholds, and procedures. This exercise should occur regularly to allow improvements to controls that are ineffective or insufficient. Although it is not possible to eradicate fraud and corruption risk, knowing where vulnerabilities exist increases the likelihood of preventing or detecting fraudulent behavior.

Implement training and other awareness initiatives

Despite frequent risk assessments and monitoring activities, an effective fraud risk management program also involves the proper communication to and training of employees to mitigate the risk of fraud in the supply chain. Organizations should develop a comprehensive training program that takes into account the risks identified in the fraud risk assessment, tailors the messaging based on individual job functions, and includes frequent touchpoints with employees to reinforce the messaging.

Continuously monitor the supply chain

In certain geographic regions, an organization's suppliers may be able to operate with little or no oversight and take advantage of schemes that are contrary to the interests of the organization. Such schemes could include the production of counterfeit goods, sale of finished goods to unauthorized parties at reduced prices, unauthorized outsourcing of manufacturing to third parties, or noncompliance with legal and regulatory requirements.

For this reason, organizations should develop programs of continuous monitoring of their suppliers. Through regular quality checks of suppliers, including unannounced visits and procedures designed to detect unusual or anomalous behavior, organizations may gain a better understanding of supplier practices. For example, examining the volume of goods rejected due to poor quality by each of the supplier's quality assurance employees might highlight strange patterns of behavior by certain of the supplier's employees. By reviewing a supplier's payroll costs and employee headcounts, organizations may identify problems caused by the underpayment of employees, overstaffing, illegal overtime, or use of child labor. By performing regular counts of the supplier's inventory, organizations may help to curb the opportunity for theft.

Including "right to audit" clauses in supplier agreements and acting on that right is the first step to effective supplier monitoring. Organizations should strive to develop best practices with regard to supply chain monitoring in order to keep these activities cost-effective and sustainable. Through continuous monitoring of suppliers, organizations may ultimately recognize cost savings through the prevention of loss or cost avoidance.

KPMG

Use data analysis

Because of the complexity and volume of transactions in today's operational environment, organizations are increasingly using data analysis to detect anomalous activity within the supply chain. Large organizations that already track the movement of goods with sophisticated IT systems may embed data analysis into existing infrastructure using software that assists in the detection of anomalies.

When an organization's general IT, payment matching, and/or transaction approval controls are weak, the organization's vendors and service providers may exploit these weaknesses by overbilling, double-billing, or submitting falsified or fake invoices. Using data analytic tools to identify patterns, outliers, and other anomalous activities can identify transactions displaying indicators of risk, and these transactions can be disseminated for follow-up through a predetermined process. Examples of these higher-risk transactions in the supply chain might include large increases in payments to one vendor, a higher volume of transactions for amounts that are just below delegated authority levels or audit thresholds, receipt of consecutively numbered invoices, or multiple invoices issued by the same vendor for work completed on the same day.

For data analysis to have an impact, organizations must have appropriate resources to follow up on the anomalies and high-risk transactions identified through data analysis. To make the best use of these resources, organizations should develop a formal data analysis methodology and procedures that help limit the number of false positives.

Ultimately, the objective of data analysis is to help the company mitigate risk and exposure. If the organization has implemented a well-designed and well-managed internal control structure to help prevent fraud in the supply chain, data analysis will be a valuable complement to the internal control structure by assisting in the detection of misconduct that does occur.

Develop an incident response plan

Often, the key to surviving a high-impact fraud is to respond appropriately upon detection of the activity rather than assuming the activity can be predicted in advance. It is important to have an incident response plan in place to allow for quick response to fraudulent activity. This plan should outline the action to be taken upon discovery of the fraud or misconduct, and it should include planning and reporting protocols. The plan should be developed with the input of Finance, Legal, IT, HR, and relevant external parties. Having such a plan helps prevent imprudent action and increases the chances of securing relevant evidence and recovering misappropriated assets.

When responding to instances of alleged misconduct, consideration should be given to conducting the investigation under the auspices of internal or external legal counsel, in order to obtain the protections that privileges offers. Additionally, organizations should develop investigative procedures that are legally and organizationally acceptable and can withstand independent third-party scrutiny. Many organizations have developed investigative codes of conduct or protocols for use in conducting investigations into fraud or misconduct. Organizations may wish to obtain a skilled fraud investigator, who can help ensure that the matter is handled properly, professionally, and in a cost-effective manner.

KPMG

High-profile issue: cargo theft

Cargo theft includes the theft of goods, money, or baggage that is part of a commercial shipment moving from, among others, a railcar, vehicle, storage facility, depot, vessel, aircraft, or distribution facility. Cargo theft is a high-profile issue for cargo owners, insurers, and the ultimate beneficiaries of the goods due to its scale and impact on the supply chain.

According to CargoNet, a national data-sharing system designed to combat cargo theft, there were over 880 reported incidents of cargo theft in the United States and Canada during 2015. CargoNet was provided a loss value on 53 percent of these cargo thefts that totaled $98 million.[9] Even more cargo thefts go unreported; in 2010, the FBI cited industry experts' estimates of losses due to cargo theft of up to $30 billion annually.[10]

Trucks and other vessels filled with goods are often unmonitored and can be moved quickly and easily. In particular, sophisticated criminals target loads that include goods of high value, those that are easy to sell, or those that meet specific needs of the purchaser of the stolen merchandise.

Cargo theft disrupts manufacturing processes, customer perceptions, and sales channels. When stolen goods appear in black markets, brand owners may not be aware that customers are purchasing their product at significantly reduced prices. If these stolen products are branded with a logo, organizations could face reputational concerns if the goods have not been properly handled, stored, or installed.

Organized crime or terrorist organizations are often involved in cases of cargo theft. These organizations may focus on shipments involving the frequent movement of cargo or those in which missing goods can go unnoticed for a longer period of time. Certain ports in the United States and globally have experienced recent increases in the volume of cargo theft. For example, ports and transportation hubs in the southeastern United States are highly targeted because of their easy access to Latin America.

To understand their risks specifically related to cargo theft, organizations should identify those shipments that have the greatest exposure to theft. When assessing these risks, an organization should consider not only the physical security of the goods but also how the internal controls could be overridden. Locks, guards, gates, fences, and cameras may present the appearance of strong security, but the security may be illusory if most issues occur after trucks leave the facility or if the theft is perpetrated by insiders. Organizations should also understand their third-party carriers, the routes that they use to transport goods, and the expected timing of shipments.

Many organizations have started using radio frequency identification (RFID) as a supply chain tool. RFID tags may be affixed to goods prior to shipment; if cargo theft occurs, the RFID tags may help to more easily track the location of the diverted goods or transport system. This technology also has significant benefits in fraud prevention as it allows for better product tracking, identification, and inventory control.

[9] CargoNet website, "2015 Cargo Theft Trends Analysis"

[10] FBI website, Archived section, "Inside Cargo Theft – A Growing, Multi-Billion-Dollar Problem, November 12, 2010

Conclusion

Supply chains are vulnerable to fraud because they are extremely complex, cross borders into emerging markets, rely on technology that can create security risks, and are susceptible to weak internal control structures. The complexity exhibited by supply chain operations allows organizations that have properly addressed and mitigated the risk of fraud and misconduct to gain a competitive advantage.

Ultimately, the importance that management places on integrity within its supply chain helps drive the measures that it takes to protect its supply chain. Such measures, including appropriate levels of due diligence on third parties, proper hiring and training of employees, and thorough risk assessments, can help to mitigate the risk of fraudulent behavior. While no risk minimization strategy is foolproof, a well-planned, well-executed, and well-maintained approach, tailored to the specific environment in which an organization operates, will go a long way to increasing the possibility of creating supply chain integrity and protecting the organization's assets and reputation.

KPMG

Contact us

Guido van Drunen
Principal, Forensic Advisory Services
T: 206-579-8107
E: gvandrunen@kpmg.com

Additional contributors:

Matthew O'Connell
Matthew F. Hansen
Sima Tavares
Kathy S. Waldrop

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.