Understanding and Mitigating Supply Chain Fraud

James L. Patterson
Western Illinois University

Kimberly N. Goodwin
Western Illinois University

Jennifer L. McGarry
Loras College

Managing fraud should be fundamental to effective supply chain risk management. Companies must maintain continuity in the face of supply chain fraud which can average about five percent of total revenue. One in seven companies will not fully recover. Minimal research outside accounting has effectively defined supply chain fraud, where it occurs, or identified best practices in mitigating and managing fraud in complex supply chain networks. Global supply chains are particularly vulnerable to fraud because of their complexity, wide dispersion, and lack of transparency, thereby making effective fraud control problematic. Internal controls are ill-prepared to protect complex global supply chains.

INTRODUCTION

Continuing to grow in both managerial visibility and executive importance, supply chain risk management (SCRM) has been defined in a variety of ways. The most general definition is deceptively simple – risk is the effect of uncertainty on objectives (A Structured Approach, 2010). As commonly defined in the literature, organizational risk includes financial, logistical, operational, and environmental, health, and safety risks. In this research, an additional source of supply chain risk can be derived from intentional fraudulent behavior and activities stemming from both internal and external sources, such as employees, managers, contingent workers, suppliers, customers, carriers, third-party logistics providers (3PLs), intermediaries, and/or consultants. Significant risk to supply chain continuity can arise from these self-seeking behavior and related fraudulent activities, striving to enrich the perpetrators while causing harm to the targeted organization.

Supply chain fraud can occur in a myriad of places along a complex global supply chain. Figure 1, "The Basic Supply Chain," is a simple pictorial representation of the different elements of a typical supply chain. Inputs include those resources, such as land, labor, capital, knowledge, technology, etc., that make up products and services produced, sold, and distributed by a company. Companies take the various inputs and transform the basic form, place, and assortment into products, services, and information that their customers value and are willing to pay for.

FIGURE 1
THE BASIC SUPPLY CHAIN

This research is grounded within the practice-based view (PBV) of organizations which is "a complementary theoretical foundation for strategic management research." As such, the PBV typically centers on an individual organization, while most supply chain activities consist of multiple entities and cross over individual organizational boundaries. Carter, Kosmol, and Kaufman (2017) describe this new perspective as the "supply chain practice view." Figure 2 "The Supply Chain Practice View" delineates the various theoretical ways of viewing an organization based on the two dimensions of "degree of imitability" and "organizational level of analysis" (Carter, et.al., 2017). The four quadrants of Figure 2 consist of: 1) resource-based view (RBV), 2) relational view (RV), 3) practice-based view (PBV), and 4) supply chain practice view (SCPV).

FIGURE 2
THE SUPPLY CHAIN PRACTICE VIEW

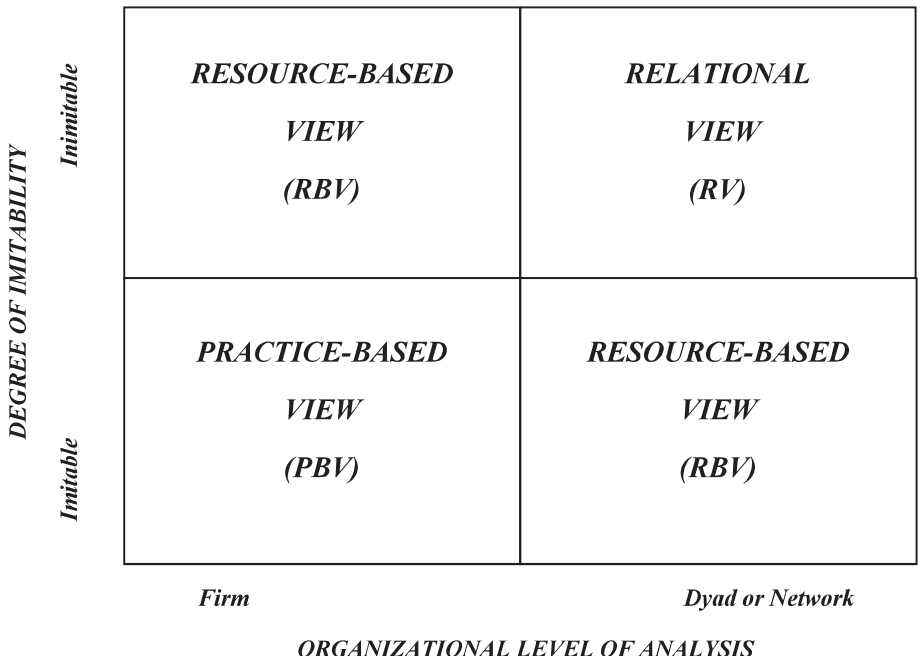


TABLE 1
AREAS OF POTENTIAL SUPPLY CHAIN FRAUD

REQUISITIONING AND PURCHASING

- **Supplier selection and management**
  - **Supplier quality misrepresentation**
  - **Bid rigging**
  - **Falsified pricing**
  - **Financial statement fraud**
  - **Supplier bankruptcy**
  - **Collusion**
- **Purchase orders**
  - **Fictitious, or dummy, suppliers**
  - **"Front" companies**
  - **Bogus intermediaries**
  - **Falsified pricing**
- **Conflicts of interest**
  - **Buyer**
    - **Ownership or other financial interest in supplier**
    - **Goods or services purchased for personal use**
    - **Kickbacks and bribes**
  - **Backdoor buying**
    - **Improper specifications**
    - **Improper relationship with supplier**
- **Conflict minerals and blood diamonds**

INBOUND TRANSPORTATION

- **Loss in transit**
- **Cargo theft**

RECEIVING, INSPECTION, AND PUTAWAY

- **Short deliveries**
- **Quantity changes**
- **Accepting damaged or low quality goods**
- **Outdated or obsolete goods**
- **Less-than-full containers, pallets, or cases**

PRODUCTION AND TRANSFORMATION

- **Counterfeit goods**
- **Substandard quality goods**
- **Setting aside of goods**
- **Product adulteration**
- **Unauthorized substitutes**

STORAGE AND INVENTORY

- **Misplaced goods**
- **Falsified counts**
- **Theft**

ORDER PICKING, PACKING, AND SHIPPING

- **Miscounting**
- **Misstated quantities**
- **Bill of lading fraud**
- **Unauthorized substitutions**
- **Theft**

OUTBOUND TRANSPORTATION

- **Loss in transit**
- **Cargo theft**

INVOICING AND ACCOUNTS PAYABLE

- **Fictitious invoices**
  - **Billing for goods and services never received**
  - **Multiple invoices for same goods and services**
  - **Billing for goods and services never received**
- **Payment fraud**

REVERSE LOGISTICS AND RETURNS

- **Removed or swapped components**
- **Theft**
  - **Goods not received back into inventory**
  - **Miscounting of returns**

GENERAL

- **Data theft or misuse**
- **Misuse of intellectual property**
- **Cybercrime**
- **Misuse of company property**

WHAT IS SUPPLY CHAIN FRAUD?

Dictionary.com defines fraud in general as "Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage." Note that fraud is not committed by accident or coincidence; it is accomplished with devious intent to enrich one's self or to deceive or harm someone else. Fraud can begin with a single, small act of subterfuge, unlikely to be discovered during normal business. However, once someone engages in several small deceptions that go undetected, the temptation to commit additional and larger acts of fraud increases as the original deception must now be maintained until the perpetrator is then trapped into an ongoing cycle of lies and cover-up.

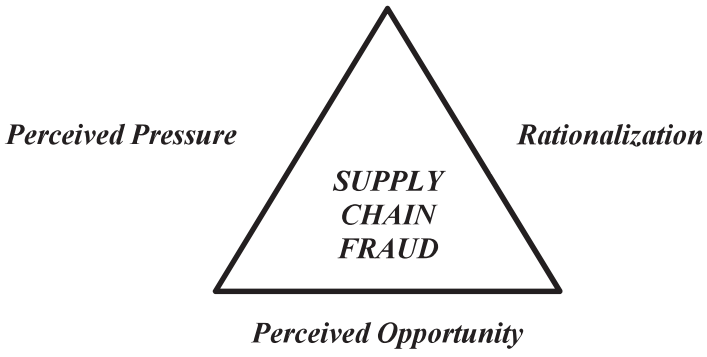
Table 1 "Areas of Potential Supply Chain Fraud" provides a greater detail of the many places in the supply chain where the potential for supply chain fraud can and does occur.

Rampant fraud could easily force a company out of business if it operates with thin margins. The Association of Certified Fraud Examiners (ACFE) states that one in seven businesses that experience fraud will never fully recover. Executives typically underestimate the level of existing fraud in their companies because they have misguided or ineffective internal control systems that fail to generate early detection of fraud, let alone the ability to detect external supply chain fraud.

A 2017 survey by Deloitte indicates that the occurrence of supply chain fraud remains high despite the increased use of supply chain analytics to detect possible fraud, waste, and financial abuse. Survey respondents indicated that the use of analytics and supply chain forensics increased from about 25 percent in 2014 to about 35 percent in 2017. More than 30 percent indicated that they had incurred at least one incident of supply chain fraud last year (Sit, 2017). According to the same survey, "[a] company does not realize that it has been a victim of supply chain fraud until it has already lost money" (Lacefield, 2017). However, Deloitte indicates that the increasing use of supply chain analytics is a solid indicator that greater numbers of companies are starting to address supply chain fraud seriously.

The pressures to commit fraud can best be characterized using "The Fraud Triangle" as shown in Figure 3 (Albrecht, Albrecht, Albrecht, & Zimbelman, 2016) and (Deterring and Detecting, 2010). The first factor involves situational or environmental pressures that place an individual in an untenable position where he/she cannot see any other reasonable way to meet one's performance goals except through extraordinary, or even fraudulent, means. Therefore, fraudulent behavior may arise when one's personal and professional goals are perceived as being unachievable via conventional means and normal levels of effort. Individuals facing goal-based pressure often feel threatened when their career advancement, income potential, or employment status is put at risk. For example, the most recent recession caused many companies to implement layoffs, thereby providing an unintended impetus for opportunistic fraud by employees. Companies struggling to meet aggressive sales and profit targets, coupled with the motivation of certain individuals to meet difficult stretch or even unrealistic goals, can inadvertently entice employees into engaging in dishonest behaviors or activities (Lehmann, 2014). Typical motivators for committing fraud included in this factor are: 1) personal gain, 2) short-term financial goals, and 3) hiding bad news (Deterring and Detecting, 2010).

FIGURE 3
THE FRAUD TRIANGLE



A second pressure factor is an opportunistic chance to commit fraud. This enables a normally honest person to consider committing fraud. These environmental opportunities can originate from: 1) a system's susceptibility to control or manipulation and 2) overarching cultural conditions that may allow fraud to occur freely. They may stem from the vulnerability of a company to a well-placed individual who is aware of points of potential weakness, including, but not limited to, a lack of internal control, non-integrated processes, an inability of employees to report questionable behavior, and so forth. Potential employees who find a company that does not perform thorough background checks and process audits could view this as an opportunity to commit fraud. ACFE has found that regular audits are credited for catching nineteen percent of fraud cases; although many cases of fraud are neither reported nor even acknowledged by victim organizations.

The third pressure factor relies on an individual's ability to rationalize fraudulent behavior in one's own mind. The underlying pressure driving much supply chain fraud often becomes the wherewithal for vindicating the individual's behavior or the company's activities for committing the actual act. However, if an organization's culture is one where high ethical standards are widely disseminated and accepted throughout the organization, it will be more difficult for individuals to justify fraudulent behavior. While it is impossible to totally eliminate this possibility, it is worth the resources committed to minimize the likelihood and associated cost of potential future fraudulent activities. In effect, this outcome could be accomplished by creating and maintaining a high ethical standard that runs from the top down in an organization. Prevention is always better than a cure (Lehmann, 2014).

WHY GLOBAL SUPPLY CHAINS ARE AT RISK FOR FRAUD

In today's increasingly far-flung, intricate, world-wide supply chains, it is often unrealistic to design and implement requisite control systems needed to efficiently monitor activities and discover fraudulent behavior (Wailgum, 2008). Differing laws and legal systems, disparate business mores, a lack of readily-available real-time data, obscured transactional details, human influence, and fluctuating demand all serve to effectively disguise fraudulent activities. Risk mapping is the intentional process of evaluating high risk areas for the potential of fraud, assessing how likely fraud is to occur, and determining and mitigating how serious its effects could be. Mapping defines a detection system of which activities are necessary to monitor on a regular basis and what follow-on actions to take, such as performing regular internal audits or more in-depth investigations into contract detail. A scoring system can then be created to analyze the probability of fraud vs. its relative impact, letting the company enforce prevention controls based on the greatest likelihood and severity (Sodhi & Tang, 2012).

As supply chain complexity continues to increase, there is a greater risk of fraud occurrence due to the greater number of links and nodes involved combined with reduced employee headcount to monitor those links and nodes. Therefore, perpetrators welcome supply chain complexity because decentralized operations make fraud detection even more problematic. Decentralization also blurs supply chain visibility in terms of assets and transactions, although visibility can be enhanced if there are clear lines of communication and expectations included with every additional link node. With increased complexity in global operations, managerial awareness of the opportunities for individuals to commit fraud is essential. Once weaknesses are identified, companies must determine the level of preventive and detective controls to implement.

GENERIC CATEGORIES OF SUPPLY CHAIN FRAUD

Fraud comes in many different forms (Coenen, 2012). The most widely recognized form of generic fraud is asset misappropriation. This occurs whenever a person, group, or entity wrongly diverts or misuses another's assets or resources for its own benefit. Typical examples include theft or misuse of money, inventory, equipment, customer or supplier lists, potential business opportunities, intellectual property, or other valuable assets, including misusing or overusing another's assets and then returning

them to their rightful owner once they are no longer needed by the perpetrator. It is a common experience that these assets are not returned in the same condition as they were when initially misappropriated.

The second general category of fraud includes a range of activities and behavior known as corruption. Although less common than asset misappropriation, the financial and disruptive impacts on a victimized company are potentially greater. Purchasing is among the top six departments where fraud is most likely to occur (Bray, 2013). Typical corruption fraud includes bribery and kickbacks, occurring when suppliers and employees collude to gain funds, personal benefits, or favorable terms of trade. Bid rigging takes place when a contract is awarded to one company without a valid competitive bid in exchange for a benefit to the buyer (Bray, 2013). Corruption can also include intentionally falsified or inflated pricing. As these schemes escalate, they typically become more readily apparent in the form of unusual or overly repetitive patterns of transactions. Corruption can be costly from the victim organization's perspective as it typically requires extensive investigation and often invites subsequent regulatory action once discovered. This fraud can result in negative public relations, as well as substantial and overtly public governmental fines and penalties.

Financial statement fraud is the third general category of fraud. An ACFE survey found that, while totaling only nine percent of cases, this is the most lethal type of supply chain fraud with losses averaging $1 million (Report to the Nations, 2014). This classification of fraud includes false financial statements and/or manipulation of accounting documents and reports that benefit the perpetrator. These occurrences show up as deliberately misstated financial records, including income statements and balance sheets, as well as quality control records, from a supplier in an attempt to win a bid or future contract. Such false statements may disguise that the supplier is approaching insolvency or otherwise incapable of performing the contract as intended. A related fraud activity involves extreme cost-cutting efforts designed to boost stock prices, increase executive perks, such as incentive pay and bonuses, and reduce cost-of-goods-sold.

TYPICAL SUPPLY CHAIN FRAUD ACTIVITIES

Fixed asset fraud is similar to asset misappropriation and often includes misuse of office equipment, company-owned or leased vehicles, computer hardware and software, and portable communications devices. Inappropriate access to proprietary and confidential information, such as client, customer, or supplier names and private information, trade secrets, strategic business plans, and budgets via electronic devices also constitutes theft of valuable intellectual property.

Purchase order fraud is a common form of exploitation and can include such activities as a buyer and supplier colluding to defraud the buyer's or the supplier's company through false pricing, inappropriate discounting, unapproved part substitution including counterfeit products, false or non-existent purchase orders, increasing quantities shipped and billed on invoices, and misleading delivery dates. While this type of fraud risk cannot be totally eliminated, organizations can largely circumvent it by segregating duties, putting effective purchasing controls in place, offering whistleblower hotlines, and setting the tone for an ethical business culture.

Trigger frauds can occur from abusing point-of-sale (POS), warehouse management systems (WMS), transportation management systems (TMS), enterprise resource management systems (ERP), and vendor-managed inventory agreements (VMI). Considering how a typical supply chain typically works, many transactions and activities are automatically initiated with minimal human oversight through the use of a "trigger event," such as an inventory item reaching its reorder point (ROP). When a ROP is reached, the inventory system triggers an automatic replenishment up to a predetermined upper limit order quantity and places the item on order. On-hand inventory quantities, or ROPs, can often be easily manipulated offline, causing early or over replenishment which can adversely affect cash flow, inventory levels, and space utilization.

Picking frauds stem from a material handler or order picker purposefully selecting a wrong item from inventory to ship to a customer or picking too much of an item and then pocketing the excess quantity for personal or unauthorized use. A customer could collude with an order picker to purposefully choose a wrong item. An unauthorized shipment of a more expensive item in place of a cheaper item can permit a

customer to inappropriately pay a lower price yet receive substantially higher value. Conversely, the customer may demand a credit on its original invoice for the wrong item received and then knowingly keep both items. This scheme works because many returned goods or reverse logistics procedures and practices are notoriously inadequate and poorly monitored.

Packing fraud occurs during the order picking process when the order picker also prepares and packs an order for customer shipment. Separating responsibility for these functions to different individuals can eliminate packing fraud unless collusion between the picker and packer exists. Additionally, the role of a clerk who enters shipment data into an inventory management system should be assigned to someone else other than either the picker or the packer.

Distribution and shipping fraud normally ensues prior to the goods being loaded onto the carrier's vehicle or container. This occurs when a material handler does not load the correct number of cases and sets them aside while falsifying the shipping manifest or bill of lading. The delivering carrier is then blamed for this short shipment by the consignee who relies on the accuracy of the shipper's bill of lading and accompanying documentation. Goods can also be misappropriated whenever the carrier loads and unloads goods at an intermediate distribution point or cross-dock facility. Bribes and kickbacks can be provided by the carrier to shipper personnel who are responsible for approving transportation contracts in order to "look the other way" for a fraudulent shipment. Another form of cargo fraud when conducted in collaboration with a supplier, buyer, or both is theft during transportation. During one nine-month span in El Paso alone, Union Pacific Railroad encountered one hundred and twenty-two robberies and eighty-seven burglaries averaging between $9-$14 million annually but hit $11.4 million in a single year (Sweet, 2006).

Receiving fraud can be promulgated by dock workers colluding with a supplier's personnel. In this case, a receiving clerk misrepresents the actual count of goods received and misappropriates the quantity difference for one's own use or black market sale. Collusion can also occur when a material handler falsifies receiving documents to hide shipment shortages from a supplier in return for a bribe or kickback.

Return fraud occurs when incorrect goods, or even legitimately ordered ones, are returned, and the returned goods receiving clerk pilfers the returned items and fabricates inventory records by stating that the returns were received but are damaged and unsalable, thereby instigating an inventory write-off for an otherwise salable or usable product. Sometimes, records could be kept accurately, but the goods can still be pilfered and not returned to stock or properly disposed.

Quality assurance fraud stems from a buyer's pressure to achieve performance goals or in collusion with an unscrupulous supplier. Lower quality, grade, or even defective goods can be substituted for normal quality or higher grade goods. Again, an unscrupulous supplier may provide bribes or kickbacks to conspiring buyer personnel. Pressure for performance may "encourage" quality personnel to stymie the normal quality assurance process by changing or ignoring approved sampling procedures or consciously overlooking the presence of inferior goods which have been substituted for regular goods. Of all the forms of fraud, quality assurance fraud holds the largest risk when it comes to consumer or public safety.

Inventory fraud is often combined with other types of fraud. This fraud is perpetrated through theft, pilferage, or misappropriation of parts and materials from a company and consists of falsifying inventory records regarding purchased, on-hand, received, or shipped quantities. The perpetrator simply allows the losses to be recorded as encountered, believing that these losses will eventually be written off during a subsequent physical inventory count. As in most supply chain fraud occurrences, the perpetrator deals in small quantities just below the action threshold which, therefore, are less likely to receive audit actions or managerial attention. The best resolution is an effective inventory management system.

Manufacturing fraud, as does quality assurance fraud, may originate through collusion with suppliers or from internal pressures to achieve overly-aggressive performance goals. The net effect is that inferior, counterfeit, or defective materials are allowed to enter the manufacturing process. Internal performance pressures may result in foregoing, omitting, or circumventing routine quality assurance inspections, allowing lesser quality goods to move directly into production without proper oversight, particularly if the line has been idled or slowed while waiting for the goods to arrive and pass inspection. U.S. companies have seen sizable manufacturing frauds with many of their foreign suppliers. There are numerous benefits

to using foreign suppliers, but without proper control and oversight, fraud's deleterious effects can be catastrophic. Even though a company may be working outside of the U.S., the overriding law is still that of the U.S., and cultural differences must be put aside to meet these standards.

Invoice-related fraud includes: 1) submitting false invoices for goods that were never shipped or 2) preparing multiple invoices for payment when only a single shipment has been received. The supplier is banking on the buyer's unwillingness or inability to challenge the fraudulent invoice(s) or overlook any discrepancy from the receiving documents. Again, buyer-supplier collusion facilitates this type of fraud. The breadth of opportunities within an organization for fraud to occur is extensive. It is unrealistic to believe that all sources of fraud within a company's supply chain can be eliminated; however, management should define and identify common fraud activities for effective risk management.

RECOGNIZING TELL-TALE SIGNS OF FRAUDULENT ACTIVITY AND BEHAVIOR

Management needs to recognize there are tell-tale signs which can indicate that something might be askew, and these signs can be categorized into four groups: 1) behavioral, 2) transactional, 3) systems, and 4) corporate red flags (Samociuk, Iyer, & Doody, 2010).

Behavioral red flags are most obvious when a person's behavior changes in unexpected ways. For example, if an employee starts spending large sums of money on luxury items, but still receives the same salary, this may indicate that there may be another source of outside income stemming from fraudulent behavior. Expensive cars, houses, jewelry, or exotic vacations are all possible indicators of fraud. In the case of bribery, excessive time spent with a supplier may indicate that the actual business relationship is questionable and should be investigated.

Another behavioral red flag may be an employee who routinely refuses to go on vacation or take time off from work. Some companies have established policies that dictate that employees must take so many vacation days off per year. Evidence of fraudulent behavior often becomes apparent if another employee covers the original person's job responsibilities during that person's time away from work. Another indicator that an employee may have something to hide occurs when an employee spends long hours at work alone after normal work hours or who refuses to work with other employees. This may also include not wanting anyone else to contact one's assigned suppliers, carriers, or customers. Employees may also repeatedly override established procedural controls to disguise their fraudulent activities.

Employees engaging in fraud may have personal problems, such as gambling or substance abuse. There are often physical indicators of such behavior, such as bloodshot eyes, lingering irritability, mood swings, or overly aggressive behavior. When such an employee is confronted with an audit, he/she may respond with belligerent resistance or attempt to deflect unwanted attention on his/her behavior and activities. In many instances, the employee provides ambiguous or intentionally misleading answers to any questions that may be raised about his/her behavior or activities, and that person may be hesitant to provide proper documentation. Another sign that an employee may be engaging in fraud is evidence that he/she is experiencing serious indebtedness or suffering from an obvious lack of money. In this case, the employee may have been tempted to engage in fraud in order to pay off debts which could be due to gambling losses, a family member's medical expenses, drug habits, or the like.

Transactional red flags consider unusual employee behavior, external relationships, or documentation of business transactions. Such activities may include doing business with companies or intermediaries that have only a few employees and/or no physical office locations. Additionally, such companies may be located in traditional tax havens, such as the Cayman Islands, the Bahamas, or Panama, or have only a post office box for its address. Also, a buyer may only be dealing with a specific supplier and refusing to consider any other suppliers. The buyer makes up excuses as to why he/she cannot use another source. Such a "preferred" supplier arrangement may be characterized by significantly higher prices than its competitors with no valid business reasoning. If large payments to overseas charities or political parties are routinely recorded, this fact could indicate the presence of bribery in other countries.

Red flags can be exhibited by a supplier. Complaints about a buyer from suppliers can provide insight into whether or not the buyer utilizes fair and competitive bidding. Also, continual poor quality from a

supplier sometimes signifies that a bribe or kickback has been given in exchange for lower quality than actually required. Changes to a contract's terms or values can indicate that the supplier may have never quoted what was actually specified. A supplier may have offered a much lower initial bid knowing that they would not comply with the terms if awarded the contract. Unusual bidding patterns may be evidence of collusion with other bidders or the buyer. For example, the supplier could be encouraging others to submit bids that far exceed its own, including: 1) competing bids sent from the same fax number, 2) similar contact information, such as name, phone, or address, and 3) comparable writing styles including similar misspellings. Sometimes, "collusive bidding" is evident when multiple bids are received that are more than thirty percent higher than estimated (Most Common Red Flags, 2014).

A common supply chain fraud involves the use of purchase orders, receiving reports, and invoices for goods that are described only in vague or relatively ambiguous terminology. This allows an unscrupulous supplier to readily substitute lower quality goods in place of higher value products. In addition, some suppliers or customers may receive undue preferential treatment without competitive bidding (Davies, 1995). Buyers must provide and follow a fair and competitive bidding process in which all suppliers are given the same amount of time and instructions to complete and submit a bid due on the same day. If a supplier is late, its bid must be discarded.

Fraudulent payments may also be made to offshore bank accounts or companies that do not exist in the company's approved supplier database. These payments are often accompanied by urgent invoices or payment instructions that seek to preclude careful review of normal terms and conditions. A crucial indicator may be use of photocopies instead of original documents with appropriate signatures. One way of enforcing this is to require that buyers attach an electronic form of the purchase order so that it cannot be easily modified. Fraudulent documents may also include false or misleading account numbers that are not normally used by or in the style of the buying company. It is not unusual for purchasing-related fraud to be virtually invisible and go remain undetected for long periods of time (Davies, 1995).

Information technology can be used to detect unusual patterns contained in billing and payment processes (Wailgum, 2008). Routine review by auditing software can identify unusual patterns of activity such as: 1) a significant increase in the number of invoices from and payments made to a single supplier, 2) an unusual number of transactions close to, but not over, maximum threshold dollar amounts that would trigger an audit review, 3) several consecutively numbered invoices from a single supplier, 4) multiple invoices from a single supplier issued on or about the same date, and 5) abnormal business transactions or approvals. Having numerous purchase orders at or near this amount should raise a warning that a supplier may be trying to circumvent the system.

Systems red flags may involve such behaviors as a key employee turning off or disabling financial controls or audit logs in order to prevent automatic review and detection of potentially fraudulent or questionable transactions or activities. Another form of this scenario occurs whenever someone logs into the system as another authorized user when that person is away from the office. A number of failed login attempts in a short time span can also indicate that an unauthorized person or entity is attempting to gain inappropriate access to a protected system. If a person is working alone after normal business hours or logs in at unusual times, this may also indicate that fraudulent activity is occurring.

Corporate red flags create undue pressure on executives, managers, employees, or contractors to engage in fraud in order to meet overly aggressive performance goals. Pressure can stem from mergers and acquisitions that have not been subjected to a rigorous due diligence process. Sometimes, managers may exercise their individual authority, making autocratic decisions about certain suppliers or customers. This may short-circuit or eliminate the normal supplier selection or customer vetting processes that are intended to prevent abuse. Also, upper management can override approved processes insisting that the paperwork already exists and will be provided later. Abuse of a friendly relationship or power can give way to fraud.

A company suffering from financial losses or declining sales margins may encourage executives or senior management to engage in inappropriate behavior, including supply chain fraud, in an attempt to improve its profit margins or hide poor business decisions from auditors, shareholders, or boards of

directors. This situation can also result from a bevy of atypical business transactions, inventory and financial statement adjustments, or post-period amendments to the company's permanent records.

A caveat is warranted here. Just because one or more red flags have been identified, this doesn't automatically mean that supply chain fraud has occurred. Legitimate and explainable reasons for the suspect behavior or activity may exist. However, it is always a good idea for a company to exercise a healthy dose of skepticism when discovering, evaluating, investigating, or auditing certain transactions, behaviors, and activities. Skepticism, as used here, is the intentional authentication of business data and information through probing lines of questioning, assessment of physical or electronic evidence with a jaundiced eye, and close attention to transactional and behavioral inconsistencies (Deterring and Detecting, 2010).

Global supply chains can inadvertently create a laissez-faire culture regarding fraud detection and effective management due to a lack of transparency and visibility. This complacency allows fraud to often proceed unabated with minimal chance of discovery. In many instances, perpetrators are discovered only when an anonymous tip points out suspected fraud (Coenen, 2012). Evaluating these tips requires the organization to thoroughly investigate the possibility of fraud, seeking to discover and remediate possible underlying gaps in its policies and procedures. However, investigations can be costly in terms of time, effort, and money. Due to the intentional nature of fraudulent activities, companies can substantially reduce fraud exposure by creating a company-wide fraud awareness culture.

SPECIFIC STRATEGIES TO MINIMIZE AND MITIGATE RISKS AND EFFECTS OF FRAUD

Two general categories of control mechanisms that can help a company minimize its potential fraud exposure are deterrence, also known as prevention, and detection (Deterring and Detecting, 2010). Deterrence controls include corporate culture management tools, techniques, and organizational development programs that provide a top-down ethical tone, as well as establishing preemptive programs. These activities should be highly visible, such that all managers, employees, suppliers, customers, contractors, carriers, 3PLs, consultants, etc. are fully aware of them and what will happen if fraud is discovered. Table 2 "Detection and Mitigation Strategies" summarizes the following control mechanisms.

Top management must develop a system of policies that are intended to prevent fraud and discover fraud activities early. Specifically, procedures must be established to prevent a single person from having access to both a transaction and the approval of that transaction, i.e., a separation of powers. Some fraud reporting processes allow anonymity to prevent possible retribution. However, senior management must be careful not to create a hostile culture or one in which they micromanage employee, supplier, and/or customer behavior. Impromptu employee interviews can provide management with information on instances that could be fraudulent, leading to more effective and timely fraud discovery.

Detection controls function behind-the-scenes, focusing on early detection and identification of potential fraudulent behavioral patterns before they escalate. Detection controls emphasize monitoring of both routine and special processes and include activities as: 1) document reconciliation, 2) cycle counting, and 3) an effective and thorough approval process. Lastly, the company should establish a system of routine internal audits that serve to highlight any activity that might be susceptible to manipulation.

According to the ACFE (Katz, 2010), the basic strategy to minimize the likelihood of fraud is a clear and distinct separation of supply chain responsibilities between individuals, such as purchasing, shipping and receiving, accounts payable, inventory management, auditing, traffic management, quality control, and sales. This is particularly acute at the lower levels of the organization. Additionally, the company needs to establish and disseminate specific policies and provide detailed work instructions that prescribe the day-to-day activities of each function in the supply chain where fraud is likely to occur. The supply chain management and accounting functions must agree to share transaction data and engage in joint activities to detect and mitigate fraud, as well as improve the reliability and consistency of the supply chain. Specifically, procurement and accounting processes must closely and routinely interleave to share relevant transaction and contract data and jointly analyze that data to ensure that the company buys, receives, and pays for only the correct goods and services it requires.

TABLE 2
DETECTION AND MITIGATION STRATEGIES

DETERRENCE CONTROLS

- **Corporate culture management tools**
- **Organizational development programs**
- **Include key suppliers, carriers, intermediaries, and customers**
  - **Know suppliers, carriers, intermediaries, and customers**
  - **Read and sign policies on fraud**
- **Appropriate policies regarding fraud**
- **Separation of supply chain duties**
- **Anonymous whistleblower policies**
- **Periodic employee interviews**

DETECTION CONTROLS

- **Monitoring of routine and special processes**
  - **Document reconciliation**
  - **Cycle counting of inventory**
  - **Thorough approval process**
- **Establish routine audits**
  - **Inventory**
  - **Contractual terms**
  - **Receiving processes**
  - **Returns processes**
- **Updated systems**
  - **Warehouse management systems**
  - **Transportation management systems**
  - **Enterprise resource planning systems**
  - **Routine electronic auditing systems**

It is also important for organizations to intimately know their suppliers and customers, especially those that are located internationally, to ensure that fictitious suppliers and customers or those located in tax haven countries do not stay in the supply or customer databases. Where feasible, buying companies should periodically examine their supplier and customer databases to check if there are problematic relationships between suppliers, customers, carriers, 3PLs, consultants, and employees that might indicate that fraudulent behavior and activities exist. In short, buyers should insist that suppliers adhere to the same sets of controls and standards to which they are subject. It needs to be clear that the supplier has a legitimate business profile and experience and that no potential conflict of interest exists with employees (Procurement Fraud, 2010).

An effective fraud prevention policy requires that all suppliers and employees read and sign an annual affidavit that fully discloses existing relationships between employees and suppliers, carriers, consultants, or 3PLs. Additionally, whenever a new supplier, carrier, consultant, or 3PL is added to the supply base, all employees who have fiduciary contact with that company must immediately disclose any relationships between themselves and the supplier. If an employee indicates that such a relationship exists, he/she must recuse himself/herself from any decision-making or contract oversight involving that supplier.

The buying company should engage in periodic audits of contractual terms and conditions to ensure that they conform to company policy and match acceptable industry practices. It is important that the buyer determine if the organization orders a particular product too frequently or in excess of normal operational requirements. The company should also periodically audit its reverse logistics and returns processes to ensure that damaged or returned goods are handled with the same level of attention and oversight as are saleable goods shipped to customers. The company should also establish policies and

procedures to ensure that damaged and returned products are scrutinized such that potential fraud can be detected and corrective action implemented.

Information technology tools can be utilized in the form of a warehouse management system (WMS) or transportation management system (TMS) to detect anomalies in the data entry process or in the scope and number of transactions. Conducting regular electronic audits and reviews can help detect suspicious patterns of transactions and payments, as well as the presence of fictitious or tax haven companies. Regarding inventory fraud, a company should establish policies and procedures for conducting routine cycle counts of key or high cost items in addition to the normal process of conducting physical counts and reconciling inventory discrepancies. The better the prevention system put into place, the less likely someone can conduct fraud. The average inventory fraud scheme lasts eighteen months until resolved.

A final fraud detection activity is establishing a comprehensive whistleblower program whereby employees, suppliers, carriers, consultants, and 3PLs could contact the company if they see or suspect fraudulent behavior or activities are taking place (Deterring and Detecting, 2010). Ideally, these programs should protect whistleblower confidentiality to protect the responder from possible retaliation. This program must be available across the entire organization on a 24/7/365 basis.

A RECENT EXAMPLE OF SUPPLY CHAIN FRAUD

In October 2017, a major industrial scandal involving Kobe Steel, Ltd. from Japan erupted with the allegation that its staff falsified key quality data regarding the strength and durability of some of its iron powder, copper, and aluminum products. This particular manufacturing fraud incident affected a variety of multinational corporations, including well-known automobile, aerospace, and railway manufacturers, totaling more than 200 customers dating back to 2007 (Suga & Mogi, 2017). At the center of this scandal, Kobe has admitted that it used non-conforming materials that were not subjected to its clients' rigorous quality specification standards. Although it is unclear whether or not any metals used by the manufacturer have resulted in specific safety-related incidents, the potential recall and replacement costs are estimated to total more than ¥15 billion or about $135 million. This monetary liability is in addition to the qualitative damage done to Kobe's reputation and its substantial estimated follow-on legal liability in damages.

Why did Kobe Steel allegedly engage in such fraudulent activity? Recalling the perceived pressure side of the Fraud Triangle, the market pressure to provide ever greater quality metals and metal alloys at lower prices in order to compete successfully in a global market could be considered the likely culprits. Customers require increasingly higher product performance with lower prices from their suppliers in order to competitive in their respective marketplaces. For example, carmakers require lightweight, yet strong, materials that are deemed both safe and fuel efficient (Kobe Scandal, 2017). Additionally, suppliers are often pressured by their customers to meet increasingly shorter and shorter lead times.

CONCLUSIONS AND MANAGERIAL IMPLICATIONS

Historically, minimal attention has been given to fraud prevention and detection in the supply chain, purchasing, and logistics literature. However, the risks, costs, and disruptions of fraud occurrence to supply chain performance can be substantial. Fraudulent behavior and related activities can often total up to five percent of an average company's revenues. Therefore, it is critical for managers and executives to better educate themselves on the types and sources of supply chain fraud in order to detect and mitigate them before they become significant.

Virtually any link or node in a supply chain can be exposed to fraudulent activity. However, there are tell-tale signs for behavioral, transactional, systems, and corporate fraudulent behavior that supply chain monitoring systems can detect and investigate to see if fraud exists. There are several scenarios that can serve to drive internal and external constituents to committing fraud in the supply chain, i.e., pressure for individual and unit performance, opportunity for fraud, and rationalizing fraudulent behavior and activities.

Fraud can never be totally eliminated, but a comprehensive auditing plan and identification program can help a diligent supply chain manager detect unusual patterns of transactions, scam or shell companies, and unusual behaviors that often denote the existence of fraud. Senior managers must also establish a strong anti-fraud culture, as well as a wide-ranging system of policies, procedures, and work instructions to send strong signals to their constituents that suspected fraud will be aggressively investigated and prosecuted. A clear separation of individual roles and responsibilities in the supply chain will also help to minimize the occurrence of fraudulent activities. Buyers must become intimately familiar with their suppliers, especially global suppliers, so that inappropriate supplier behaviors are discovered and the offending suppliers removed from the supply base.

REFERENCES

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2016). *Fraud Examination*, 5th edition, Boston: Cengage Learning.

Bray, J. (n.d.). Watch for These Types of Purchasing Fraud. *Accounting Software by Cougar Mountain*. Retrieved from http://www.cougarmtn.com.

Carter, C. R., Kosmol, T., & Kaufmann, L. (2017). Toward a Supply Chain Practice View. *Journal of Supply Chain Management*, 53, (1), 114-122.

Coenen, T. L. (2012). Are Your Employees Committing Fraud?. *CFO*, Retrieved from http://www3.cfo.com.

Davies, D. (1995). Purchasing and Procurement Fraud. *Journal of Financial Crime* 2, (4), 322-30. Retrieved from http://www.emeraldinsight.com.

Deterring and Detecting Financial Reporting Fraud: A Platform for Action (2010). Washington: Center for Audit Quality.

Katz, N. (2010). Protect Against Procurement Fraud. *Inside Supply Management*, 21, (3), 16.

Kobe Scandal Shows Cost of Race to Keep Improving Metals. (2017). *Bloomberg: Industry Week.* Retrieved from http://www/industryweek.com.

Lacefield, S. (2017). More Companies Are Using Analytics to Detect Supply Chain Fraud, Says Deloitte. *Supply Chain Executive Insight E-Newsletter*. Retrieved from www.supplychainquarterly.com.

Lehmann, D. (n.d.). Watch for Fraud in the Supply Chain. Deloitte. Retrieved from http://www.deloitte.com.

Most Common Red Flags of Fraud and Corruption in Procurement. (n.d.). The World Bank Group. Retrieved from http://siteresources.worldbank.org.

Procurement Fraud: Investigative Techniques to Help Mitigate Risk. (2010). Deloitte Development, L.L.C.

Report to the Nations on Occupational Fraud and Abuse – 2014 Global Fraud Study. (n.d.). Association of Certified Fraud Examiners. Retrieved from http://www.acfe.com.

Samociuk, M., Iyer, N., & Doody, H. (2010). *A Short Guide to Fraud Risk*, Farnham, UK: Gower Publishing.
Sit, S-S. (2017). Supply Chain Fraud High Despite Analytics Use. *Supply Management*. Retrieved from https://www.cips.org.
Sodhi, M. S., & Tang, C. S. (2012). *Managing Supply Chain Risk*. New York: Springer. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000* (2010). London: The Association of Insurance and Risk Managers, Devon, UK: The Public Risk Management Association, and London: The Institute of Risk Management.
Suga, M. & Mogi, C. (2017). Steel Firm Faked Data for Metal Used in Planes and Cars. *Bloomberg*. Retrieved from https://www.bloomberg.com.
Sweet, K. M. (2006). *Transportation and Cargo Security: Threats and Solutions*. Upper Saddle River, NJ: Pearson/Prentice Hall.
Wailgum, T. (2008). Fraud and Theft Risks in Global Supply Chains Are Everywhere. *CIO*. Retrieved from http://www.cio.com.