The McHard Firm
933 San Mateo Blvd NE, Suite 500-501, Albuquerque, NM 87108
1220 Rosecrans St, Suite 102, San Diego, CA 92106
505/554-2968 NM 619/764-6144 CA 877/279-2942 Fax

Procurement: Common Requirements and Weaknesses

Janet M. McHard, Founding Partner, CPA, CFE, MAFF, CFF

Insert course objectives here

Procurement fraud can generally be classified under two types of schemes: internal and external. Internal schemes are being perpetrated by people within the organization, while external schemes are perpetrated by people outside of the organization using methods such as bid-rigging. There are also hybrid types, including people both inside and outside the company, which includes things like bribery, corruption, and illegal gratuity.

Internal schemes are more likely to be caught by internal accountants. External schemes, on the other hand, are generally more difficult to detect and investigate, and may potentially incur larger losses than an internal scheme. However, a hybrid scheme can completely degrade the internal controls of an organization and result in massive losses. To begin the course, let's discuss some of these types of schemes.

Billing Schemes

Billing schemes are an example of an internal scheme. Depending on the type of organization, the **purchasing cycle** (how an organization purchases inventory and/or supplies on a regular basis) can be one of the largest expenses an organization has, along with payroll. The difference between them for a fraudster is that, depending on the organization, payroll is generally a consistent cost from month to month. The purchase of inventory and supplies, however, can change a great deal, which can be exploited by a fraudster.

The number and amount of variation in transactions in the purchasing cycle makes it easier for a fraudster to slip in fake transactions without being noticed. Invoices can be fabricated to appear legitimate; a process made much easier with the aid of technology and the widespread use of emailed invoices.

Using this type of scheme, the fraudster doesn't have to worry about physically taking money from a cash register or stealing inventory, or being caught on camera while performing fraudulent actions.

Finally, this process also generates unwitting accomplices. When a fraudulent invoice comes in, if the person approving the invoices would be considered an unwitting accomplice if they approved the fraudulent one. When it comes time to generate checks to pay those

© The McHard Firm

© The McHard Firm

invoices, the person who generates the check for the fraudster could also be an unwitting accomplice.

Many times, the fraudster will accomplish such a scheme by billing an organization for a good or service that was never performed, either with a legitimate company name that hasn't provided anything to the payee organization, or with a fictitious or "shell" company that the fraudster has created for this purpose. Another common tactic is for a company to bill twice for their goods or services. If done intentionally, this can be an example of a billing scheme fraud.

Sometimes, a fraudster will call the bank the organization uses and, by pretending to be a representative of the organization, can change the information on a payment so that it goes to them instead. This is one reason why organizations must maintain tight internal controls on who is authorized to change such information.

Personal purchases using a company credit card or company funds can also be a source of fraud. In other cases, a fraudster may alter existing purchase orders or requisitions to order more inventory than the company needs, which they can then sell on the side for more profit, or return to the vendor for cash or gift cards.

So, how would an organization or investigator go about detecting a billing scheme? A good place to start is by investigating vendor complaints. Having an anonymous tip line for such complaints, and making sure the vendors know about it, is important in order for investigation to follow. You can also investigate unusual payees, or any other details that seem out of the ordinary when it comes to vendors or the purchasing cycle.

Performing site visits of vendors can also be helpful, as well as site visits to the departments of the organization that are making purchases or processing payments. Particularly in large companies, fraudsters will take advantage of geographical distance to hide their actions, so performing site visits can help to prevent fraud.

Analyzing computer records and data records, such as checking for addresses that match between employees and vendors, can also help detect false invoicing and the like. You can also keep an eye out for unusual activity in "soft accounts", which are accounts that exclusively have services going through them, meaning no physical goods or merchandise, or any account with words in it such as: suspense, miscellaneous, "to be researched", or temporary. These kinds of accounts aren't as predictable as others, which can allow a fraudster to conceal their fraudulent transactions.

In some cases, increased payments to specific vendors can also be a warning sign, particularly if that vendor has some kind of relationship or connection to someone in the organization.

Internal audits or investigations can often benefit from their position by using payroll and HR records to investigate employee lifestyle changes, such as living beyond their means. If you notice a high volume of activity for a fairly new vendor, that may also warrant some investigation.

© The McHard Firm

External Fraud Schemes

External fraud schemes are so named because they are committed by outsiders, rather than an employee or member of the organization, and they attack both the business and the consumers. External fraud tends to be more difficult to detect than internal fraud, because as the perpetrators are not operating from within the company, any documentation or records that may provide clues don't reside with the victim organization. This makes it more difficult for investigators to obtain accurate, reliable records to investigate, as the outside vendors (even if they aren't committing fraud) may be unwilling to share records with investigators.

One way to make this less of a problem from an internal controls standpoint is to include an **audit clause** in contracts with the vendors, before any suspicions of fraud arise.

When outside vendors are the ones committing fraud, it often takes the form of **bid-rigging,** which is when a group of potential vendors discuss beforehand what result they want the bidding to have and influence it thusly. This can include **bid rotation,** when vendors take turns winning certain bids; **bid suppression,** when vendors decide that certain people shouldn't bid on certain offers; and **complimentary bids,** when vendors try to change the available contracts so that more than one vendor can be hired.

External fraud can also take the form of **market division,** where vendors or companies divide the market between themselves. For example, each vendor may get a zip code in which they bid, guaranteeing they get all of the business in that zip code so long as they don't bid in someone else's. There is also **price fixing,** where vendors will collectively decide the price for a good or service, generally higher than market value, so that contract offerors will be forced to pay that higher price as no one is bidding below it.

Overbilling schemes also occur, wherein the vendor bills their client for more money than they should be. Sometimes this can be caught by internal controls, but not always, and at first will start small and snowball over time. As with internal fraud, external fraud can also involve shell companies, and can be detected by similar analysis.

Luckily, there are warning signs and way to look out for vendor fraud. Once again, a primary source of information are complaints from employees and other vendors. An anonymous complaint line provides a place for people to complain in a way that feels safe.

Other than complaints, many ways of detecting vendor fraud comes down to recognizing patterns in how vendors are bidding. A vendor re-bidding after being rejected with only a few very specific changes to win the bid, especially if those changes wouldn't be immediately obvious to someone outside the company, may be an indication of attempted fraud.

If you've had a standard bid price among your vendors that suddenly drops when a new vendor comes along, this may mean that your previous group of vendors were colluding to keep prices high.

© The McHard Firm

If there are qualified contractors out there that are refraining from bidding, it may be an indication that the vendors who are bidding for that service are enforcing bribery or bid-rigging, which the contractor doesn't wish to be involved with. Interviewing that contractor about their decision not to bid may be helpful to determine if something fraudulent is occurring.

If you've noticed contractors who seem to always, or perhaps seem to never, bid against each other, it may warrant investigation. It's possible that they have some kind of side agreement regarding who is allowed to bid on which contracts.

If the successful bidder on a contract proceeds to subcontract to a losing bidder, particularly if the winning bidder has some aspect that makes them preferable (such as being in-state, owned by certain people, etc.), this can be a clue that the successful bidder is actually a subsidiary of the other company. This strategy raises the chance that the larger company will still see some profit even if they don't win a bid. If you notice a pattern to the winning bidders, this could also be a red flag.

You can also detect possible fraud by paying attention to the wording of the bids. If you notice different bidders making the same math or spelling error, this could be an indication that multiple bidders are being run by the same people.

Bidders changing their prices at the same time, especially when materials cost or other factors wouldn't be a factor, could imply that the bidders are collaborating on their bids.

A big red flag is if you notice a pattern of the winning bid always being the last to bid. This can be a sign that someone on the inside could be telling the winner what the lowest bid is so that they can undercut it.

On an invoice from a vendor, if you are receiving consecutive numbered invoices that are unbroken, this could mean that you are that vendor's only customer, which in turn could be evidence that the vendor is a shell company owned by an employee or other associate. If invoices are consistently just under the cost threshold for higher review and approval, or if an employee is splitting purchases into more than one transaction to keep them under the level for review, they could be trying to conceal fraudulent actions.

A decline in the quality of goods received from a vendor can also be a clue, as when vendors are paying kickbacks, they oftentimes will overprice certain goods, reduce the quality of the goods, or decrease the quantity of the goods in order to make up for it. If kickbacks are being paid, that may be reflected in the records as unusual or one-time extra charges.

As with other types of fraud, an employee having unexplained lifestyle changes, or evidence that they're living above their means, can be an indication that they are getting extra funds from somewhere.

© The McHard Firm

Hybrid Schemes

Hybrid schemes involve perpetrators both inside and outside the organization, or collusion between vendors and employees, and can make an investigation even more difficult, as you have multiple perpetrators working to conceal the fraud, as well as increased profit loss due to multiple people stealing at the same time. In addition, many of the records you would normally rely on to prove intent, and therefore fraud, aren't in the possession of the victim organization, making information gathering difficult.

Bribery is a very common example of hybrid schemes, including things such as kickbacks, bid-rigging involving employees, and illegal gratuities. This kind of scheme can also be called **corruption.**

What is the difference between a bribe and a kickback? Simply put, a bribe is paid before the event or actions, and a kickback is paid after the event; in the case of procurement schemes, these are often paid to an employee within the organization who will direct business to the vendor paying them. As discussed earlier, this can take the form of bid-rigging, having a predetermined bid winner, bid rotation, pre-bid communication with a specific party, or splitting purchases to avoid RFP limits. Sometimes it's as simple as choosing the company that will provide the best kickback or bribe.

An illegal gratuity is also given after the transaction occurs, sometimes much later, and may include non-cash considerations like offers of future employment or below market interest rates. What is interesting about illegal gratuities is that if it influences an official act from a governmental organization, intent does not need to be proven to declare it an act of illegal gratuity.

Some red flags to look for when investigating corruption are the repeated use of the same vendor, especially if there are other vendors who could provide the same service. You can also look for any unusually close relationships with vendors, which often will come from a tip, and once again, for a suspect living beyond their known income.

There are many ways that bribes, kickbacks, etc., may be paid. They can be made in cash, paying off a credit card or purchasing a prepaid credit card for the insider, offering gifts, travel, or entertainment, payments to offshore accounts, payments to the family members of the insider, or a share of the paying company's business.

Another kind of collusion scheme is known as **conflicts of interest,** wherein an employee has undisclosed interests that compete against those of the organization. Being undisclosed is important, as sometimes if the conflict is fully disclosed and appropriate controls are instituted, it may be allowable. When investigating such a conflict, look for evidence of personal gain from the related parties to ensure that it has been fully disclosed and that the appropriate controls are in place.

© The McHard Firm

Procurement References

In the United States, the Department of Justice has a manual that includes a unit on procurement fraud. In section 9-42.420, Federal Procurement Fraud Unit, under the 9-42.00 Fraud Against the Government section, the manual states:

> *That unit… handles a variety of fraud cases affecting both civilian and defense agency procurements, including product substitution, false testing, cost mischarging, defective pricing, and kickback cases. … The Unit provides expertise and guidance on procurement fraud issues to investigative agencies and United States Attorneys' Offices that request their assistance.*

What this means is that if you have a large fraud case in this jurisdiction, you can request the assistance from this unit; this is particularly useful when an investigation reaches the point of prosecution, as the unit can assist in finding a prosecutor for the case. Many such cases are prosecuted through what is known as the False Claims Act, one section of which is particularly important for an investigator:

> *31 USC §3729 False Claims (a)(2)(D): has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property.*

The key word in this section is *knowingly*— in order for this law to be used for prosecution, you must prove the suspects intent, as with other kinds of fraud. In another section of law, 18 USC §1001 Statements or entries generally, it states that lying, concealing, or providing any kind of false information to a federal investigator is a prosecutable crime. 18 USC §1031 Major Fraud Against the United States is where a large portion of white-collar crime and procurement fraud are prosecuted under, which also emphasizes intent.

18 USC §201 Bribery of public officials and witnesses outlines the law for bribery. However, in the United States, this law only applies to a public or government official. Bribery of any other kind of organization may be a crime under state law, but is not a federal crime. 18 USC §371 Conspiracy to commit offense or to defraud the United States is often invoked when a case involves more than one fraudster.

Many white-collar crimes at both state and federal level invoke 18 USC §1341, which defines fraud in regards to mail and wire fraud. This means that the fraudster used some sort of physical delivery system, such as the US Postal Service, or wire system, such as email, to further the fraud.

Conclusion

There are many ways fraudsters can use the procurement system for their own benefit. In this course we have considered the most common forms of procurement fraud, what parts of the system are weak to fraud, and what signs you can look for to detect fraud. With these tips, you will be well-prepared to investigate procurement fraud cases in the future.

© The McHard Firm

Glossary:

Bid-rigging: When a group of vendors discuss ahead of time what they want the bidding to look like, and influence it thusly.

Bid rotation: When vendors agree to take turns winning bids.

Bid suppression: When vendors agree that certain companies shouldn't bid on certain contracts.

Complimentary bids: When vendors try to alter existing contracts so that more than one vendor may be hired.

Conflict of interest: When an employee has fiduciary duties to more than one organization.

Corruption: Collusion from persons both inside and outside an organization to commit fraud, often through use of bribes, kickbacks, and illegal gratuities.

Market division: When vendors use some metric, such as zip code, to divide the market between them and guarantee no competition in certain areas.

Overbilling scheme: When a vendor overcharges an organization for goods or services.

Price fixing: When a group of vendors decide the price for a resource, good, or service, generally higher than the market value, to enforce a uniform higher price.

Procurement fraud: Fraud which uses procurement, or how an organization purchases goods and services, for personal gain.

Purchasing cycle: How an organization purchases inventory or services on a regular basis.

© The McHard Firm