QUICK GUIDE ON PROCUREMENT FRAUDS

SAVE YOUR ORGANIZATION BEFORE IT'S TOO LATE!

$2.9 TRILLION

THE POTENTIAL GLOBAL LOSS DUE TO PROCUREMENT FRAUD.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS.

INDEX

OVERVIEW

Prevention is better than cure, and it is very critical for organizations to identify the areas of risk to protect themselves from incurring losses. Sometimes an organizational fraud can even cost an arm or leg to an organization.

Bribery, conflicts of interest, fabricated paperwork, counterfeiting, and tax evasion are some of the few terms that we never relate with the procurement function. But in reality, frauds can occur at any stage of an organization. And while procurement plays a critical role in working with third-party supply partners, an increased focus on the impact of supply chain disruption has elevated the level of that engagement — driving significant corporate investments to enable strategic risk assessment and mitigation.

It's incorrect to assume that all supply chain-related exposure initiates outside of the organization and that procurement's role is limited to monitoring and response planning. A myopic focus on external risk also overlooks the fact that fraud and corruption in procurement are common enough that all companies must take steps to protect themselves. This is particularly true since the increased use of technology has facilitated distributed buying, moving an increasing percentage of procurement activity outside of the procurement function.

In this paper, we will draw a framework and discuss areas associated with the fraud. We will also talk about specific scenarios that lead to enterprise exposure and what steps procurement can take to mitigate related risks.

> Because procurement is a complex operation involving large sums of money and multiple contractors, it is highly vulnerable to fraudulent schemes.

- Rob Biedron

THE REASON BEHIND FRAUDS

> **If you think that a fraud may be happening then fear the worst.**
>
> *- Ken Frost*

Unlike "grey area" activities that are usually covered by corporate ethics standards and governance policies, procurement frauds involve intentionally deceptive behaviors that enable an individual, team or supplier to benefit at the expense of the enterprise knowingly. The fact that the actors are all willing participants also increases the likelihood of them taking steps to conceal their wrongdoing, making it even harder for the enterprise to uncover and address truly undesirable behaviors.

The reason to commit such a crime could be numerous, which could include perceived opportunity without consequence coupled with greed, desperate need of money, other financial opportunities, benefitting family members, or friends. Even though the reasons could be many, the after-effects of these frauds are costly to the company.

To prevent this a "right way" of doing things should be established. Procurement may document detailed governance policies that outline specific expectations for buyer and supplier behavior, but even more important is the establishment of the expectations and principles that underlie all spend management activity. These include the idea that the enterprise has the right to determine which suppliers will be the source of specific goods and services, what the company will buy from those suppliers, how much they will pay for each purchase, and which channels are approved for making said purchases. Anyone that accepts the justification behind the existence of corporate procurement must also acknowledge that – when spending corporate resources – the final authority belongs to the enterprise.

1

Frauds related to Supplier Selection

Supplier Selection is one major area where procurement frauds can occur. The risk of fraudulent supplier selection ranges from the contracts resulting from the strategic sourcing process to individual supplier selections made to meet each business need. Regardless of the scale of the selection, when buyers knowingly disregard which suppliers the company wants the business to be conducted with and the process by which those suppliers are selected, the result is a fraud. Given the pervasive role of technology in supplier selection, users may have to make a significant effort to skirt established processes, eliminating questions about their intent and making it possible for procurement to monitor this activity through automated reporting and systems audits.

1.1 Bid Rigging

Bid Rigging is an illegal practice in which competing parties collude to choose the winner of a bidding process while others submit uncompetitive bids. Bid rigging stifles free-market competition, as the rigged price which will be higher than what might have resulted from a competitive bidding process. The main objective of bid-rigging is to increase the amount of the winning bid. In the case of bid-rigging, most of the frauds are detected are at later stages, when the company must have almost lost its market share.

Recognizing the signs of possible bid-rigging is key to deterring it. Those who handle procurement processes should be on the lookout for warning signs or “red flags.” They can further **take steps to reduce the likelihood** of wrongdoing. Some of the ways to do it are as follows:

- **Establish a Bidding Pool**
  Maximize the number of bidders, know the supplier and market prices, keep bids confidential.

- **Drafting Tender Specifications**
  Require disclosure regarding potential subcontractors and their pricing, avoid preferential treatment for a certain class of suppliers, avoid predictability—consider aggregating or disaggregating contracts.

- **Awarding Contracts**
  Avoid splitting contracts between suppliers with identical bids, establish a complaint mechanism for suppliers to voice competition concerns and ask questions if prices or bids don't seem to make sense

- **Training and Auditing for those who handle procurement processes**
  ensure regular staff training on bid-rigging recognition, review tender history and results periodically

- **Conduct interviews**
  Conduct interviews with vendors who no longer offer supply / unsuccessful vendors.

Case Study on Bid-Rigging

In the 1950s, manufacturers General Electric and Westinghouse conspired to fix prices for industrial products in a case that involved both price rigging and bid rigging, as well secret meetings to pick winning and losing bids for orders in which winners rotated based on phases of the moon. It was uncovered by the Tennessee Valley Authority upon reviewing identical bids over many years in what were meant to be secret bidding processes. It resulted in fines and jail terms for companies and individuals involved.

Source: https://www.investopedia.com/terms/b/bid-rigging.asp

1.2 Faulty Approval Authority

Fraud Detection

- Perform audits of supplier award rationalization, supplier capabilities and delivery or quality history
- Analyze No PO / No Pay compliance reports to identify non-compliant users
- Analyze purchasing card and T&E transactions to identify non-compliant users
- Generate reports to monitor buying patterns, volumes and timing
- Monitor small purchase orders (close to or just under established approval thresholds) looking for end users "sourcing" repeatedly from the same supplier
- Run PO approval reports by the user to spot unusual approval patterns
- Regularly review approver lists to determine that assigned permissions match each user's current role

In most organizations, each stakeholder is granted a specific level of approval authority based upon their role in the corporate hierarchy. This authority is usually associated with a specific dollar value per purchase, designed to create alignment between the individual's responsibilities and the permissions they can give. Users with a significant level of approval authority in their hands could expose the enterprise to risks while appearing to adhere to governance procedures.

Fraud Prevention

- Ensure end-user involvement in sourcing projects to reduce the incentive for maverick buying
- Establish and maintain a No PO / No Pay Policy
- Communicate procurement policies and penalties to employees and suppliers
- Define specific use cases for purchasing card usage and monitor closely for exceptions
- Maintain spend thresholds which control the majority of spend
- Review tail spend looking for opportunities to consolidate it into managed or contracted spend
- Guide end users to approved suppliers to encourage compliance
- Ensure that HR-maintained hierarchy data matches the system approvals and interfaces with the S2P solution
- Ensure that "delegated" approvers understand the budget ramifications of that status

Case Study on Faulty Collusion between Parties

In 2005, a global technology company opened an internal investigation into one of their midlevel supply managers. They found evidence on his company-issued laptop that he was sending confidential information about product road maps, design specifications and pricing goals to suppliers. That information was then used by the suppliers to ensure their proposals were both the most competitive and maximized their opportunity for profit through targeted negotiating leverage. In return for this ill-gotten information, the manager received bribes from the suppliers. As a result of his actions, he faced both criminal and civil suits. After pleading guilty in court, he had to surrender all of the ill-gotten funds, owed thousands of dollars in additional fines, and faced the potential of prison time. Although these consequences focus on the supply manager's behavior, they cannot come close to reflecting the extent of loss of funds, supplier performance, and intellectual property experienced by the company during his tenure.

GOOD READ

Fraud training significantly reduces the loss—businesses that trained managers and executives reduced loss by 55.9% and those that trained employees reduced it 51.9%.

Source: https://www.amanet.org/articles/protect-yourself-against-fraud-in-procurement/

2

Frauds related to Product Pricing, Costs and Spends

Even though today's contract life-cycle management platforms bring detailed contract terms into close contact with even the most distributed purchasing activity, there are still ways that suppliers with ulterior motives can accept purchases that do not conform to contracted prices and quantities. Although the information is available to track these critical details, most approval frameworks are designed to monitor permissions and compliance at the PO or invoice level rather than at the line-item level. The combination of the item price and quantity in each purchase creates two separate opportunities for fraud and therefore requires more significant investment in oversight.

2.1 Compromising the quality of a good

The strategic sourcing process emphasizes the need to document specifications as well as aids in negotiating prices. If there are changes in any of them, the net effect can result in an escalation in pricing. When quality is degraded while prices remain the same, suppliers are fraudulently overcharging customers. Unfortunately, because deliveries continue to be made on time, procurement may not catch this type of fraud right away — at least until downstream users and customers complain of the altered product or service quality.

2.2 Expense Reimbursement

Expense reimbursement fraud continues to plague procurement departments, costing organizations thousands of dollars in lost revenue every year. According to a recent study, this type of fraud, which includes filing false claims for reimbursement on fictitious or inflated business expenses, costs a median loss of $40,000 every year. Employees who are claiming reimbursement account for about 14% of all asset misappropriation sub-schemes at companies, according to the report. Expense reimbursement schemes typically go on for two years before the organization detects them. The longer a fraud lasts, the more money an organization loses.

2.3 Demand Data Mismatch

Fraud Detection

- Analyze pricing against product quality to flag items that fall out of the expected range
- Analyze spends to track transactions and flag risks, exploring all automated options to maintain procurement efficiency
- Compare spend patterns and volumes with supplier reports to validate internal spend numbers
- Monitor purchasing records for evidence of orders deliberately split to circumvent approval thresholds

Procurement relies heavily upon spend analysis to ensure compliance, manage demand, and monitor budgets, but it is not the only valuable source of "truth." Reports should be regularly compared to the data available from suppliers to ensure that price and quantity match the expectations of both organizations.

Fraud Prevention

- Involve procurement in the approval and monitoring of contracts with premium and nonpremium pricing
- Include in the documentation of all contract terms that buyers and suppliers are both accountable for price fluctuations

Did you know?

Top fraud expenses organizations incur include:

- 5% of a typical organization's annual revenues are lost due to fraud
- 83% of fraud cases involve asset misappropriation, including padding T&E claims
- $154,000 is the median loss from asset misappropriation

- Tina Gunn

3

Frauds related to Invoicing

Invoice fraud happens when a company or organization is tricked into changing bank account payee details for a sizeable payment. Criminals pose as regular suppliers to the company or organization and will make a formal request for bank account details to be changed.

3.1 Inflated Invoices

Inflated Invoices typically mean the prices or amounts mentioned in the invoices are higher than agreed upon sums. Supporting paperwork, such as the purchase order, might make it clear that the company ordered or offered to pay a particular amount. And yet the invoice charges more, suggesting invoice fraud.

Example of Inflated Invoices

A seller may list the cost of goods at $100, but the actual cost was $50. The buyer pays a higher price without knowing the true cost.

3.2 Duplicate Invoices

Another type of fake invoice scam is when an organization is asked to pay for duplicate invoices, even when it only received a product or service once. A simple sign of a duplicate invoice is getting more than one invoice for the same goods or services. The invoices might even have the same date, purchase order number and invoice number, making it clear the invoice was also received at least once. This is also done so that the organization would see these invoices as evidence where multiple payments were made on the same invoice by the person who sent the invoice and is hence demanding to be paid again.

Fraud Prevention

- Always verify details of any new/amended payment instructions verbally by using details held on file, and not on the instruction. Fraudsters can spoof email addresses to make them appear to be from a genuine contact, including someone from your organization.
- Look carefully at every invoice and compare it to previous invoices received that you know to be genuine – particularly the bank account details, the wording used and the company logo.
- Consider setting up single points of contact with the companies you pay regularly
- Regularly conduct audits on your accounts
- Make all staff aware of this type of fraud, particularly those that are responsible for making payments.

CONCLUSION

Purchasing fraud can and does happen to the biggest companies on the planet, and several government examples are legendary. The key to prevention is understanding the data, the change in market prices, and the trend in purchasing patterns. This proactive approach is powered by the continuous audit of transactions, comparison of data from different applications, and comprehensive tracking of process.

It is also important to know that the cost of fraud is not just limited to financial loss, but also increased risk, wastage of an organization's resources and an unproductive decision making. Frauds, more often than not, lead to public image disruption for an organization. The stakeholders lose their trust and as a consequence, the company may have to pay a higher price for credit. They may be refused membership in trade associations or might be blacklisted for a strategic alliance.

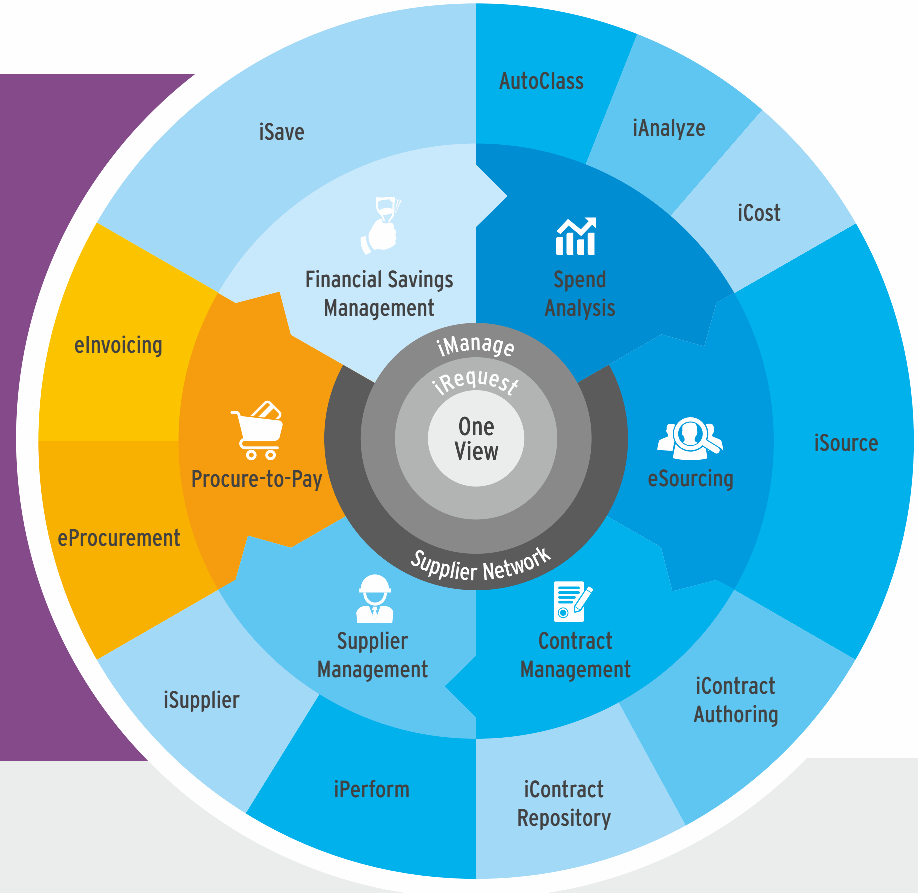
The consequence does not end here, and it affects the reputation of the employees too. This is more pronounced in small firms where the employees are more connected with one another. Auditing costs also increase, as auditors would scrutinize the company thoroughly before signing any financial statements.

The only way to suppress all of these is by focusing on logistics of how cash enters and exits your organization. An increased awareness between both the suppliers and buyers could be an effective measure too. With strict policies and organizational workflows, an organization can maintain its market position, which could gradually help in building up the image, further facilitating increased revenues and market share for the organization.

✦ ✦ ✦

ZYCUS™

Zycus is a leading global provider of complete Source-to-Pay suite of procurement performance solutions. Our comprehensive product portfolio includes applications for both the strategic and the operational aspects of procurement - eProcurement, eInvoicing, Spend Analysis, eSourcing, Contract Management, Supplier Management and Financial Savings Management. Our spirit of innovation and our passion to help procurement create greater business impact are reflected among the hundreds of procurement solution deployments that we have undertaken over the years. We are proud to have as our clients, some of the best-of-breed companies across verticals like Manufacturing, Automotives, Banking and Finance, Oil and Gas, Food Processing, Electronics, Telecommunications, Chemicals, Health and Pharma, Education and more.



USA	**:**	**Princeton:** 103 Carnegie Center, Suite 321, Princeton, New Jersey, United States, 08540 | Ph: 609-799-5664 **Chicago:** 5600 N River Road, Suite 800 Rosemont, IL 60018 Ph: 847-993-3180 **Atlanta:** 555 North Point Center East; 4th Floor, Alpharetta, GA 30022 Ph: 678-366-5000
UK	**:**	**London:** Kajaine House, 57-67 High Street, Edgware, Middlesex HA8 7DD, United Kingdom Ph: +44(0)1189-637-493
ASIA	**:**	**Mumbai:** Plot No. GJ-07, Seepz++, Seepz SEZ, Andheri (East), Mumbai - 400 096 Ph: +91-22-66407676 **Pune:** Pride Purple Accord, 1st Floor, Above Vijay Sales, Next to Hotel Mahableshwar, Baner Road, Pune - 411045 Ph: +91-22-66407676 **Bangalore:** MFAR Silverline Tech park, Unit No. 2, 3rd Floor, Plot No. 180, EPIP Area, 2nd Phase Whitefield, Bangalore 560066 Ph: +91-80-46737676 **Singapore:** 101 Cecil Street, #20-11, Tong ENG Building - 069533
AUSTRALIA	**:**	**Melbourne:** Level 9, 440 Collins Street, Melbourne VIC 3000
MIDDLE EAST	**:**	**Dubai:** Unit EX - 20 , Building No 12, Dubai Internet City, Dubai , UAE, PO BOX No. 73000