

The Future of Fraud Prevention in Procurement

Introduction

Corporate fraud is often associated with sophisticated cyberattacks, data breaches, and hackers infiltrating organizational systems. While cyberfraud can pose serious and potentially devastating risks to businesses, procurement fraud remains one of the most prevalent forms of corporate fraud. According to the global survey findings published in the ACCA Policy & Insights report, "Combatting Fraud in a Perfect Storm," procurement fraud has a 34% global prevalence rate and a 35% materiality rating, highlighting its significant impact on organizations.

Procurement fraud can occur at various stages of the purchasing and supply chain process, from supplier selection and tendering to contracting, invoicing, and payment. Given that procurement is fundamental to acquiring the goods and services required for day-to-day operations, weaknesses in procurement controls can expose organizations to financial losses, reputational damage, operational disruptions, and regulatory risks. Consequently, strengthening procurement governance, transparency, internal controls, and oversight is essential for organizations seeking to safeguard resources and maintain integrity throughout their supply chains.

Understanding the Procurement Fraud

Procurement fraud is an occupational crime. Association of Certified Fraud Examiners (ACFE) defines occupational fraud as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources. Procurement fraud generally falls into two main categories under the ACFE Fraud

Tree: asset misappropriation and corruption.

One of the most common forms of asset misappropriation is a billing scheme. Under this scheme, a business is deceived to make payments for unprovided services or unsupplied goods. Normally, the ghost vendors or shell

companies are used to execute such schemes. Another way is using the Company's credit card or purchasing channel to buy items for personal use.

The corruption is the second most important category. According to the ACFE, corruption occurs when an employee abuses his position or influence for personal benefit, in breach of his duty. In procurement, this often involves manipulating the supplier selection process through practices such as bid-rigging and kickbacks.

Why Procurement Fraud is Hard to Detect?

Unlike a cyberattack, which can trigger sudden security alarms, procurement fraud is often difficult to detect because it is designed to look normal. In Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques by Bart Baesens, Véronique Van Vlasselaer, and Wouter Verbeke, this behavior is compared with the camouflage techniques used by animals such as chameleons and stick insects. Abdelrahim Al Aqqad, in Fraud Analytics in Action, also discusses this "camouflage effect." Fraudsters deliberately imitate normal business behavior so that their actions blend in with legitimate employees and routine transactions. The figure 2 provides a brief snapshot of the procurement cycle along with potentially fraudulent activities that look business as usual.



Mumtaz Hassan, FCMA
Financial Controller
Nishat Mills Limited

Figure 1: ACFE's Occupational fraud and abuse classification system (The Fraud Tree)

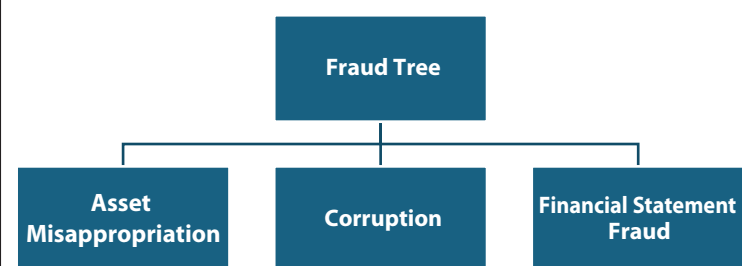
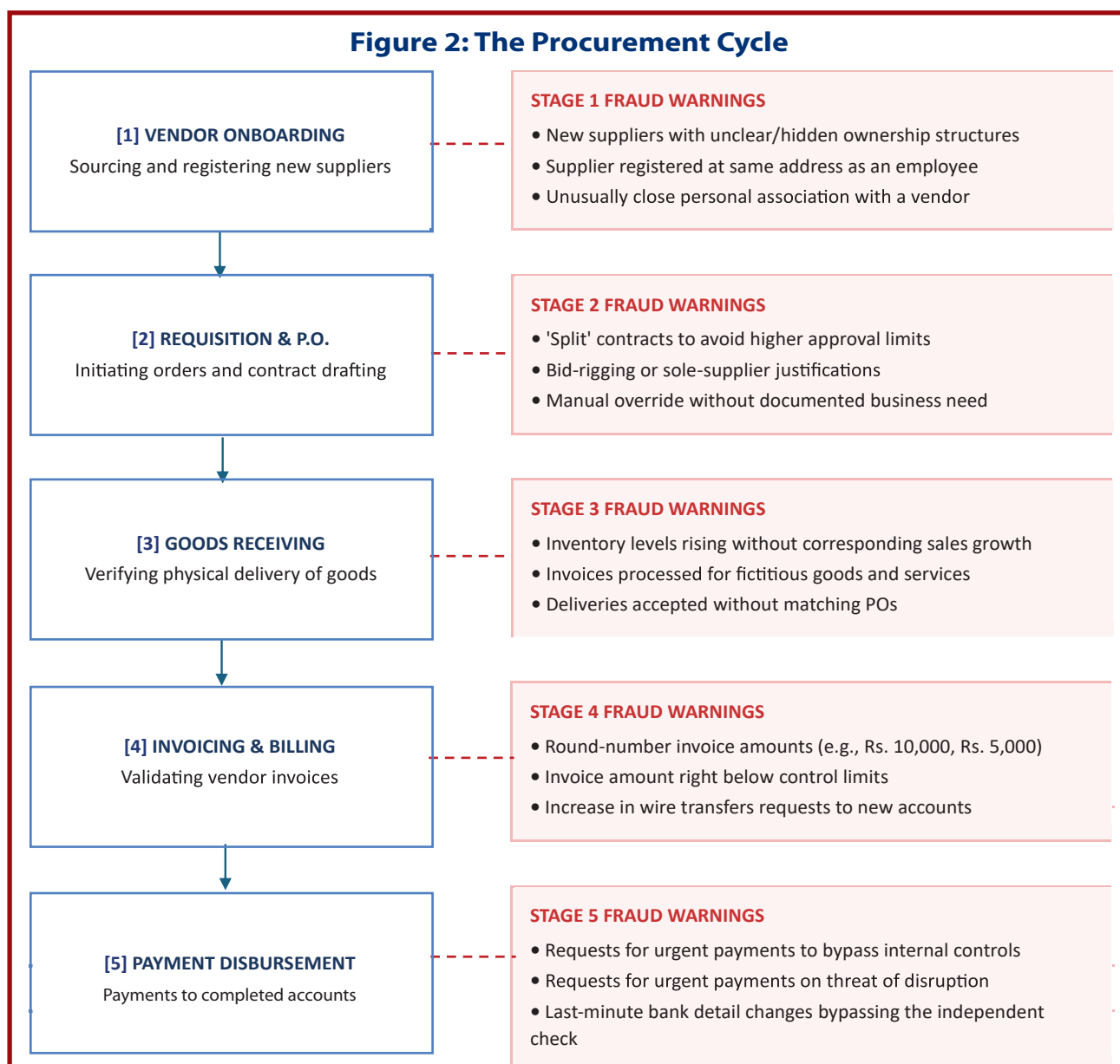


Figure 2: The Procurement Cycle

AI and Machine Learning: The New Smoke Alarm

As discussed above, a procurement fraud can blend into normal business activities which makes it hard to detect. Moreover, in this age of information technology millions of transactions can take place at very high speed without the use of a single piece of paper making human supervision difficult. Therefore, businesses need tools that can sense small signs that humans may overlook. In this regard, Artificial Intelligence (AI) and Machine Learning (ML) can play an important role.

Detecting Anomalies in Real-Time

Under a traditional audit a sample of invoices and transactions is checked and verified after these have

already been processed. On the other hand, an AI system can continuously analyze large volumes of transactions in real-time processing. It helps to identify unusual patterns on the go. The unusual transaction times, repeated round-number transaction or other abnormal patterns can easily be identified and flagged. For example, Accenture has integrated an unsupervised AI-based anomaly detection model into its corporate expense reporting system. This solution continuously screens 100% of expenses to isolate statistical outliers i.e. unusual expense claims and hidden patterns of non-compliance. This system has significantly reduced the auditors' time and enabled them to utilize it for investigating the suspicious transactions flagged by the AI.

Learning What is Not Normal

Machine learning can identify unusual behavior even if the exact fraud pattern has never been recorded before. Traditional systems normally depend on predefined rules such as flagging the transactions above a certain amount. The fraudsters can immediately learn these rules and make plans to circumvent them. Unsupervised ML can learn abnormal behavior and identify deviations from the normal pattern. This is highly useful when methods of fraud are changing and evolving. For example, Master card, a global payment network uses AI, ML and anomaly detection software to identify transactions which deviate from normal customer behavior. Since anomaly detection does not rely only on previously marked fraud examples, it can identify new fraud patterns which never happened before.

Natural Language Processing: Reading Between the Lines

The clue for fraud is not merely hidden in numbers. This can be found out in emails, letters, agreements and other written communications. Natural Language Processing (NLP) can help to detect fraud in these sources. NLP can be used to analyze large amounts of unstructured data to identify unusual words, themes, patterns and relationship e.g. unclear and evasive words such as "usually", "normally", "perhaps", "generally". These words may provide a sign that the person communicating about a transaction is trying to mislead. This may not detect a fraud but provide a lead to a suspicious scheme. The American Securities and Exchange Commission (SEC) has realized the importance of language and uses an NLP software which is designed to read between the lines for detecting the probability of fraud in the communication of executives of the companies.

From Finding Fraud to Connecting the Dots

AI's strength is not limited to finding an instance of fraud in isolation such as in a single transaction or a single account. It can connect many signals, which is necessary, because modern fraud schemes depend on relationships between people, device, and accounts. Therefore, an important analytical shift has happened from simply "finding fraud" to "connecting the dots" through artificial intelligence and Social Network Analysis (SNA). The complex entities and their interactions are modelled as network graphs through SNA which shifts the analytical lens from individual behaviors to overall relational structures. For example, a procurement manager again and again awards contracts to the same supplier. The supplier's invoices



are always below the approval limits. Accounts Department pays immediately. Moreover, the supplier's registration records are linked to another employee's personal business entity. Although, all these events seem harmless in isolation. But, an AI system can analyze the hidden relationships and find out the fraud scheme.

Blockchain and IoT: Building a Trusted Supply Chain

Businesses have become complex. A transaction normally involves many employees from multiple locations interacting with various suppliers while engaging outsourced logistics. This is also done through scores of digital systems. It makes traditional security systems unreliable. Therefore, the businesses have to install checks on devices, individuals and systems along the way as transaction or event proceeds. Blockchain and Internet of Things (IoT) are helpful and create a "digital mirror" of what is taking place physically.

Creating a Digital Mirror of Physical Operations

The Blockchain and IoT are used to capture information about goods as these are moved through the supply chain. For example, if a transporter installs telematics devices or trackers in his trucks, he can have timestamped record of the location, and movement. This can be used to trace the goods. It may also be used to review a claim of a disgruntled client in case of a dispute about the delivery of goods happens.

Blockchain: Creating a Shared Version of the Truth

While IoT is helpful in knowing what is happening physically, blockchain makes it possible to record and save this information digitally in Trustworthy way. A shared blockchain ledger can be used to record information collected by sensors of IoT. The entries in the blockchain ledger cannot be changed without authorization after these are properly recorded and validated. This highly reliable record can be shared with confidence among buyers, suppliers, transporters or any other party.

Connecting Physical Goods with Financial Transactions

The Blockchain and IoT can together effectively prevent ghost transactions and issuance of fake invoices. For example, a seller dispatches 10,000 meters of fabric to a garment factory. Suppose, the goods were never delivered to the factory. The documents like purchase order, delivery challan, inward gate pass and invoices were fake because of all relevant persons colluded.

The accounting system might have recorded the purchase of goods even though these were never delivered.

However, if the IoT have been employed, the digital mirror of the physical movement of the goods would have been recorded automatically. Additionally, blockchain could have saved the information in a tamper-resistant record. This record can be verified with the physical record and in case of tampering, fraud would be detected.

Creating a Culture of Integrity

The role of technology is very important in preventing fraud, still the human factor cannot be ignored in fraud detection. The businesses should promote the culture of ethics and integrity among employees.

Shared Accountability

Accounts, IT and Internal Audit cannot solely be held responsible for fraud prevention. Since fraud can happen anywhere in the organization, fraud detection and prevention are the shared responsibility of procurement, operations, IT, accounts, internal audit etc. These functions must regularly communicate and share information about possible fraud risks. It is worth noting that fraud normally happens where systems and work of different departments meet with each other. In fact, these are fraud detection points; therefore, communication among these departments is vital.



The business should establish anti-fraud steering committees. The members of such committee should be from various departments across the organization such as finance, operations, risk, IT and Internal Audit. This diversified representation will bring different perspectives on fraud risk evaluation and prevention.

Creating Safe Channels for Speaking Up

It is easier for an employee to notice the unusual behavior of his or her colleague. Any wrong such as giving favor to a particular vendor, posting of fake invoices or suspicious phone calls of a colleague can be easily sensed by other colleagues. However, employees hesitate to report even sometimes very obvious signs. They don't want to risk their careers for fear of retaliation. Moreover, if unproven after investigation, they would be regarded as troublemakers.

The business should establish channels that are confidential and safe for the employees. A formal whistleblowing policy should be implemented under which employees should be able to raise their concerns on more than one channel but anonymously.

Visible Action

The ethical culture can strengthen only if the outcome of investigation is communicated keeping all the necessary information confidential. The organizations may publish and circulate newsletters on "speak-up outcomes" preferably on quarterly basis. These should discuss the concerns raised, investigation done, corrective actions taken, and lessons learned. The objective of this communication is how seriously the concerned raised were considered without naming the individuals involved. This should be done without discrimination ensuring that the same rules also apply to senior and high-performing employees.

Becoming a Hard Target

The fraud can never be eliminated fully because bad people filter through the organizational hierarchy. Such people are also normally happened to be very creative, adaptive, and tech savvy. Still, a combination of AI, blockchain, IoT and ethical culture can make an organization a hard target for the fraudsters. They go away for easier targets when they realize that an organization is actively searching for anomalies and asking the right questions.

About the Author: Mr. Mumtaz Hassan is a Fellow member of ICMA and currently working as Financial Controller at Nishat Mills Limited.