WHITE PAPER

A How-to Guide for Preventing Procurement and Payment Fraud

Tips for reducing risk and protecting hard-earned profits

Fraud Happens

Though accounts payable teams have always had to contend with fraud, today's scams seem to be more sophisticated and more costly than ever before. One example: The FBI recently arrested a cable TV executive on charges of defrauding his employer of more than $8 million. He is alleged to have initiated contracts for services with companies he owned, for services that were never delivered, while using false and stolen identities to mask his involvement.

You may think "it can't happen in my company," but you might want to think again. According to the Association for Certified Fraud Examiners (ACFE) *2020 Report to the Nations*, the typical company will lose 5 percent of annual revenues to fraud. Data from the Kroll *Global Fraud & Risk Report* for 2019-2020 shows that 28 percent of companies globally fell victim to fraud by external parties, and 27 percent fell victim to fraud by internal parties.

Fraud Can Come From Everywhere

28%

affected by external fraud

27%

affected by internal fraud

According to the Kroll Global Fraud & Risk Report 2019-2020

How Fraud Is Introduced

Both procurement processes and payment processes are vulnerable to fraud.

On the procurement side, fraudsters can set up "phantom" vendors that exist in name only, hoping they will escape your controls and can make their way into your vendor master. Typically insiders are involved in these phantom vendor schemes and will personally approve purchase orders, vendor master changes and payments.

Another variation involves what can best be described as business-level identity theft. The fraudster sends legitimate-looking correspondence or makes a personal phone call to request bank account or address changes that will redirect payments intended for one of your suppliers.

Similarly, insiders can take advantage of stale accounts. They can identify aged open service POs that contain outstanding balances, submit a bank account change and then submit fraudulent invoices against the PO for amounts below standard matching tolerances.

Fraud can also enter your business on the payment side of procure–to–pay. Someone simply submits a fake invoice and hopes it will escape close scrutiny. Often an unsuspecting payables clerk will simply create a vendor record so the invoice can be paid.

Seven Lock-Tight Tips for Halting Fraud

Regardless of the source of the fraud or how sophisticated the perpetrator, there are things you can do to regain the upper hand and protect your hard-earned profits. Follow the tips below and you'll be well on your way to reducing your risks.

01 Use a Supplier Portal for Change Control and Risk Management

How many times does your accounts payable team get phone calls or email messages asking you to change a bank account number, payment address or a point of contact? How do you verify and track the change to ensure you aren't being scammed?

It's a time-consuming and risky business to make changes directly into your vendor master file. One of the most effective alternatives is to adopt a supplier portal for secure, self-service registration. When you do, you will have a single source for the truth about your vendors—and one that is highly controlled and automatically vetted before anyone gets paid.

You can require suppliers to enter their business name, address, bank account information, tax ID number and other critical information before they are ever added to your vendor master. Any portal worth its salt should automatically validate critical information in real time using public and private databases—ensuring that fraudsters can't masquerade as a trusted supplier. Discrepancies are flagged and must be resolved before registration can proceed.

Any changes made after the initial registration can be accomplished only by someone with the supplier's login and password. What's more, the portal captures a comprehensive audit trail of each login, the changes made and approvers—enforcing segregation of duties, dual control and other compliance rules along the way.

02 Close Stale POs and Vendor Master Records

A PO that remains open after a vendor has completed work for your company is the equivalent of cash left on a table. The PO, which was meant to control spending and prevent fraud, provides an easy path for fraudulent transactions to slip through.

Institute regular screening for inactive POs and vendor records and close them as soon as possible. Close POs that have reached 90 percent of value after 60 days of inactivity, and all POs after no more than six months of inactivity. Close vendor records after no more than 13 months of inactivity.

03 Tighten Your Payment Approvals

Sometimes the simplest controls are the most often overlooked. According to the apexanalytix Compass™ Benchmarking Survey, nearly half of companies fail to require a second approval on large payments. While most of us are eager to reduce touchpoints and to streamline procure-to-pay processes, the risks involved with large payments are simply too great to ignore. Having a second set of eyes review information before a large payment is released simply makes good business sense.

04 Compare Supplier Information to Employee Records

The ACFE *Report to the Nations* 2018 contains eye-popping statistics on the cost of occupational fraud. When employees are involved, the median loss is $150,000. In nearly one out of every four instances of employee-related fraud, losses will top $1 million.

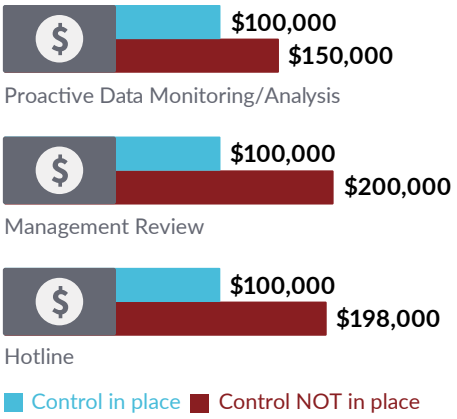
It is clear that codes of conduct and whistle-blower hotlines simply aren't enough. You need other control methods if you want to reduce your risks.

Fortunately there are alternatives. Today you can adopt sophisticated fraud detection software that will compare employee records against your vendor master to spot any overlap. If a phone number, address, bank account number or other supporting details are found in both, you'll be able to investigate and intervene.

Do fraud detection solutions make a difference? According to data from ACFE's *Report to the Nation 2020*, the answer is an emphatic yes. Companies adopting tools for proactive data monitoring and analysis average a nearly 33 percent drop in fraud losses.

Fraud Controls

Organizations lacking anti-fraud controls suffered greater median losses



Source: ACFE, Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse.

05 Focus on Patterns and Common Fraud Attributes

Certified fraud examiners know there are distinct patterns and attributes that can signal a fraud scheme is lurking. Examples include high-risk addresses and countries, consecutive invoice numbers, small first invoices to test the waters, and use of private mailboxes that mask the absence of a physical business address.

This is another area where fraud detection software really shines. It can help you uncover patterns and anomalies that would be nearly impossible to spot during a manual review.

You can use these powerful fraud detection tools in two ways. First, you can continuously and proactively monitor your procure-to-pay systems to prevent losses before a payment is disbursed. You can also perform a retroactive audit to uncover and halt fraudulent activity you might have overlooked in the past. One large retailer using detection software for a retroactive analysis found about 40 fraudulent vendors who had scammed the company for tens of millions in revenue before they were discovered.

06 Adopt an E-invoicing Solution

Moving away from paper invoices and adopting e-invoicing or other automated or self-billing invoice methods can give you much greater control over an important entry point for costly billing schemes. Most invoice automation initiatives begin with an approved vendor list, which reduces the risk of spurious invoices being used to create a vendor record. As with a supplier portal, only certain authorized individuals are able to access the e-invoicing system in order to submit invoices. Once a supplier is on an automated invoicing method, reject invoices submitted through any other pathway.

07 Move to Direct Deposit

Most companies adopting e-invoicing do so in lockstep with an automated clearing house (ACH) or other electronic payment initiative. With electronic payments, check tampering becomes a thing of the past. Direct deposit eliminates manual touchpoints and gives you a secure transmission path directly from your company bank account to that of your supplier.

Take an Integrated Approach

There is no single solution to safeguarding against fraud. Instead it's best to take an integrated approach and to do lots of things well. Adopt the right technologies. Tighten your process controls. Look back to uncover fraud that might already be embedded, and look forward to halt potential new scams before they can take hold. The risks are simply too great to ignore.

To Find Out More

If you would like to learn more about how to protect your company from fraud, contact apexanalytix experts at +1 800-284-4522.

An integrated approach

- Adopt the right technologies
- Tighten your process controls
- Uncover fraud that's already embedded
- Prevent new scams before they happen

About the Author

Aiesha McLeod is the Account Manager for Vendor Risk Compliance with apexanalytix and is a member of the firststrike Consulting group, which implements and supports apexanalytix software for clients. In this role she manages vendor risk engagements, educates clients on third-party risk, evaluates vendor data, and provides recommendations in support of client fraud risk and compliance initiatives. She is a financial compliance professional with over 20 years of Accounting/Finance experience in multiple industries and has expertise in improving internal controls and conducting fraud investigations. Prior to joining apexanalytix, she worked as a Financial Compliance Analyst with focus areas in fraud investigations, fraud risk assessments, compliance program management, and compliance training. Aiesha holds a BA in Accounting from Savannah State University and a BA in Management Information Systems from Saint Leo University. Aiesha is also a Certified Fraud Examiner (CFE).

Americas Headquarters
1501 Highwoods Blvd., Suite 200
Greensboro, NC 27410-2047
+1 800-284-4522

EMEA Headquarters
Exchange House, 494 Midsummer Blvd.
Milton Keynes, MK9 2EA
United Kingdom

APAC Headquarters
Suites 2701-3, 27/F, AXA Tower, Landmark East
100 How Ming St., Kwun Tong, Kowloon
Hong Kong