WHITE PAPER

Is Your P2P at Risk for Fraud?

Six signs your company's procure to pay
is at risk and what you can do about it

The Corporate Fraud Epidemic

The impact of fraud on today's businesses and organizations is staggering. Just take a look at these examples pulled from headlines.

- The former head of digital fraud and security for the international Lloyds Banking Group was charged with defrauding his company of more than £2.5 million by creating false invoices and pocketing the income.
- Two employees of the U.S. Army Corps of Engineers pleaded guilty to a scam involving $30 million in payments made to bogus companies they created.
- Authorities in China arrested 18 people in a crackdown on an alleged invoice forgery ring; they confiscated more than 2.5 million fake invoices.

The activities of such fraudsters can be tough to detect—especially by companies with far-reaching global operations and multiple shared services centers. In its *2020 Report to the Nations*, the Association of Certified Fraud Examiners (ACFE) says the typical organization loses 5 percent of its revenues to fraud each year—an estimated $4.5 trillion industry-wide.

Most scams last a median of 14 months before being detected, ACFE says, and only about 1 percent of them are uncovered via IT controls in the U.S. What's more, almost half the organizations that fall victim to fraud fail to recover their losses.

Nowhere is the risk greater than in the procure-to-pay cycle, which represents the largest annual outlay for most companies. The ACFE says internal control weaknesses were responsible for nearly half of frauds. Fraudsters simply follow the money. Often the perpetrators are trusted employees who are familiar with internal financial controls and know how to fly beneath the radar.

Here's just one example of how it can happen. A member of the accounts payable team for a Fortune 50 company billed her employer by establishing her brother as a fake vendor and paying him $9,999 weekly. The invoice amount was one dollar shy of the $10,000 limit requiring a second authorization. This well-orchestrated fraud put the employee on track to net more than $500,000 a year.

Do you have a fraudster on your own team?

4.5T

The typical organization loses 5 percent of its revenues to fraud each year—an estimated $4.5 trillion industry-wide.

14

Median number of months most scams last before being detected.

50%

Internal control weaknesses were responsible for nearly half of frauds.

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

Signs Your Organization Could Be a Victim of Fraud

While there can be dozens of potential tip-offs that a fraud scheme may be underway, here are six of the most common that you should definitely have on your radar screen.

1. **Employee-Vendor Matches.** Overlapping vendor and employee data, such as a mailing address or phone number, can signal that your own employees are conducting fraudulent activity.

2. **Initials in the Vendor Name.** Fraudsters use this technique to mask their true identity and to make it difficult for them to be found or identified if the illegal activity is discovered.

3. **High-Risk Countries.** Statistics show fraudulent transactions often can be correlated with countries scoring low on Transparency International's Corruption Perception Index and known to be havens for entities involved in fraud, money laundering and other corrupt practices. Ranking the lowest in the 2019 list are Somalia, South Sudan, Syria and Yemen followed closely by Venezuela, Sudan, Equatorial Guinea and Afghanistan which tied for being the fifth most corrupt countries.

4. **Consecutive Invoice Numbering.** It is unlikely a vendor is providing goods or services to other customers if the invoices you receive are numbered consecutively. If you are the only client, fraud may be the likely reason why.

5. **Small First Payments.** Fraudulent vendors who want to test your internal controls often will submit a small initial invoice, followed by larger amounts once they are firmly established in your systems. Look carefully for this suspicious pattern.

6. **Round Amounts.** With a few exceptions in professional services, invoices generally have dollars and cents. Summing to total rounded or even amounts is unlikely, but happens more frequently when contrived invoice amounts are created.

Why "Sampling" Is Not Enough to Uncover Fraud

Uncovering fraud in accounts payable can be a complex undertaking. It is virtually impossible for large companies to manually screen each vendor record and each invoice for fraudulent trends and anomalies—especially before disbursements are made. Instead, many organizations try to sample accounts payable data at some regular interval or after the fact.

Though sampling for signs of fraud is helpful, be forewarned that it has serious limitations. Experience shows the greatest potential for fraud is at lower spending limits where businesses have the largest number of vendors and invoices. That means huge data sets are needed for sampling to be effective. Both the time and expense involved are simply beyond the reach of most organizations.

How Audit Software Reduces Your Fraud Risk

To reduce costs and improve the thoroughness of fraud screening, many companies are turning to software-based tools that analyze all data—not just a sample. These systems are specifically designed to review your vendor and employee databases and invoice activity company-wide for high-risk characteristics—from vendors and employees who share the same mailing address to invoice or payment amounts that fail to match expected patterns.

Companies can use these powerful fraud detection tools in two ways. First, they can perform a retroactive audit to uncover and halt fraudulent activity overlooked in the past. Many find they recoup their investment in the software with this single data sweep.

The results can be heart stopping. One example: A large retailer used detection software to analyze 100,000 vendors and rank the 100 most risky. Subsequent investigations confirmed that approximately 40 percent of the top 100 were indeed problematic, representing tens of millions in lost revenue.

In addition to retroactive audits, fraud detection software can be used to intervene and prevent losses proactively. A data delimited file is pulled from each payment platform and analyzed for anomalies before payments are issued. The software produces an easy-to-use report ranking risky vendors and invoices by the level of threat they represent.

With data at your fingertips, you'll be poised to further investigate potential fraud or policy violations and can intervene to protect hard-earned revenues. These same reports can be used to uncover systemic process weaknesses so you can shore up controls and policy enforcement.

Reducing Fraud Investigation Time

With the detailed case information that software and user analysis can produce, you also can shorten the time it takes to investigate fraud—readily answering the typical questions an investigator would ask.

A large global retailer using fraud detection software and risk analysis procedures, reduced investigation time from 12 weeks to just three days. That meant the retailer's internal investigation team had time to pursue more suspected instances of fraud and could protect tens of millions in revenues that otherwise would have been lost.

What to Look for in Fraud Detection Software

If you want to add automated fraud detection to your arsenal, look for a solution that adheres to industry best practices. Here are a few of the important features of best-in-class software:

- Reviews all data routinely, not just a sample.
- Provides a continuous auditing framework—from supplier setup through invoice reconciliation.
- Analyzes a wide range of vendor and invoice attributes right out of the box, without the need for costly software development.
- Easily extracts the data to be analyzed from all types of payment platforms, whether commercially available or developed internally.
- Compares employee data to vendor files and payment information in order to spot internal collusion.
- Raises an alert if transactions involve countries perceived to be a high risk for corrupt practices.
- Provides actionable results packaged in concise, easy-to-read reports that rank potential risk, minimize the number of false positives and capture the information you need to intervene.
- Supported by a company that invests in ongoing product development and evolves its analytics to keep up with savvy fraudsters.

Flexible Deployment Models

You also should look for a solution backed by a vendor who offers flexible deployment models. That means you will have the flexibility to integrate fraud monitoring into your accounts payable operations in a way that works best for you. Industry leaders will offer these options:

- **Fraud detection software as a cloud-based, managed service.** On-demand subscription pricing options and virtually limitless capacity can help you quickly respond to changing business needs.
- **Fraud detection incorporated into a recovery audit.** If you're not ready to invest in fraud detection software or to sign up for a managed service, you can look for a recovery audit partner who incorporates fraud detection software into the recovery audit process.

One caution: There are a number of popular enterprise resource planning and management solutions that support accounts payable operations. Don't be lulled into thinking these systems are enough to help your company detect and prevent fraud. They aren't set up for that purpose and don't have the in-depth capabilities required to get the job done. Instead, look for a solution especially tailored for the task at hand.

To Find Out More

If you would like to learn more about how to prevent fraud at your organization, contact apexanalytix at +1 800-284-4522. To assist in your comprehensive approach to protecting your company, you may also be interested in the apexportal® Supplier Registration module with features such as bank account ownership validation.

About the Author

Michele Arndt is the Executive Manager of Global Software Consulting at apexanalytix with extensive experience in accounts payable, post-audit services and software for imaging and audit. She is former director of document management and client services and a former director of accounts payable for a large retailer. Michele is a founding member of the IAPP board, has been a contributor to Paytech, and is active in the Institute of Financial Operations.

apexanalytix revolutionized recovery audit with advanced analytics and the introduction of firststrike overpayment prevention software. Today, apexanalytix leads the world in supplier management innovation with apexportal and smartvm, the most popular supplier onboarding and compliant master data management solution available. With over 250 clients in the Fortune 500 and Global 2000, apexanalytix is dedicated to providing companies and their suppliers the ultimate supplier management experience. To learn more visit www.apexanalytix.com, email apexinfo@apexanalytix.com or call +1 800-284-4522.

apexanalytix®
Ultimate supplier management™

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