corcentric

Proven results. *Built together.*

WHITEPAPER

The Ultimate Guide to AP fraud detection and prevention: the *new* mandate for modern business

Introduction: *The unseen threat to your bottom line*

In today's fast-paced business landscape, Accounts Payable (AP) fraud has emerged as a critical threat that organizations can no longer afford to ignore. As remote work becomes the new norm, traditional controls have crumbled, leaving businesses exposed to increasingly sophisticated fraud schemes. AP fraud has skyrocketed to the top of the list of challenges faced by financial departments, outpacing even the demands for timely payments and transparency. One thing is clear: the piecemeal approach to combating this menace is a thing of the past. In this guide you will find a robust strategy to mitigate AP fraud, leveraging experts, automation and cross-functional alignment to stay ahead of evolving threats.

The cost of AP fraud is on the up

It may be no surprise to you that businesses are bleeding cash when it comes to fraud. Invoice fraud alone siphons off an average of $300,000 per year in the US[1]. Fraud eats up roughly 5% of annual revenue, with the typical case inflicting a median loss of $117,000 over 12 months before it's caught[2].

Whether you're big or small, the problem persists. For corporate giants raking in $10 billion or more, 52% have faced fraud in the past two years, and 1 in 5 of these companies endured a hit exceeding $50 million[3]. Small businesses aren't faring any better—they're 42% more likely to get hit by fraud than their larger counterparts[4].

Expense fraud is another silent killer, making up 15% of all reimbursements. And it's not just paper trails—58% of accounts payable (AP) departments fell victim to business email scams in 2021[5].

These numbers don't just highlight a problem; they scream it. AP fraud is a silent but significant drain on businesses, regardless of size and industry.

New ways of working bring new exposures

Accounts Payable Fraud (AP fraud) is rapidly evolving into a high-stakes game where the lines between physical and digital threats blur. Once a predictable risk, it's now a complex web of internal and external manipulations targeting an organization's payment systems. Fraudsters are getting more sophisticated, whether they're employees, vendors, or cybercriminals.

Classic schemes like invoice fraud—tampering, duplicating, or fabricating invoices—are being

[1] https://www.prnewswire.com/news-releases/medius-us-businesses-lose-on-average-300-000-per-year-due-to-invoice-fraud-301641518.html
[2] https://snappt.com/blog/fraud-cost/
[3] https://www.pymnts.com/news/b2b-payments/2023/incoming-payments-fraud-costs-companies-millions-every-year/
[4] https://snappt.com/blog/fraud-cost/

supercharged by technology. The rise of fictitious vendors draining company funds has never been more prevalent, but it's just the beginning. For instance, Business Email Compromise (BEC) is the new darling of AP fraudsters, tricking companies into rerouting payments to unauthorized accounts. Meanwhile, old-school tactics like check theft and payment change requests still haunt businesses, often leading to devastating financial losses.

The landscape of AP fraud is shifting, and staying ahead of these ever-changing threats is no longer just a necessity—it's a battle for survival. As Brittany Carmichael, a Corcentric StopFraud Client Services Supervisor points out,

"Our team validates all new supplier profiles that come through the system. They go through our twelve-step validation process upfront, and then we also validate and monitor any sort of updates that come across for a supplier's company, such as to their company information or their payment information."

Going back to the example of email, once the go-to workaround for managing supplier onboarding and invoice approvals, it has now become a prime vulnerability. Here's why relying on email can present a risk to your AP department:

- No chain of custody: Emails lack the built-in security to track every hand that touches an invoice.
- Weak separation of duties: Without robust enforcement, a single breach can compromise multiple stages of the AP process.
- Zero transparency: Email doesn't log actions, leaving you in the dark about invoice status.
- Deletion risk: Invoices can disappear without a trace, leading to payment gaps and unauthorized transactions.

As AP departments grapple with these challenges, the risk of fraud balloons, especially in a decentralized work environment where control is harder to maintain.

The anatomy of AP fraud

Accounts payable fraud is evolving into a sophisticated arena where unscrupulous actors—both inside and outside the organization—exploit cracks in payment processing systems to siphon off funds. Let's break down the key categories of this growing threat.

Internal Fraud Schemes

These are the wolves in sheep's clothing, where insiders (employees) leverage their positions to pull off fraudulent activity. Here's how they do it:

- False expense reports: Employees fabricate or exaggerate expenses for reimbursement.
- Supplier collusion: An employee teams up with a supplier to submit inflated invoices or bill for phantom services.
- Check theft and tampering: This old-school scam involves forging signatures, altering check amounts, or outright stealing checks to redirect funds.
- Billing schemes: Employees set up fake vendors or inflate invoices, sneaking illicit payments into their own accounts under the guise of legitimate transactions.
- Fictitious vendors: Ghost vendors are created by insiders, who then greenlight payments, gradually draining company funds.

Internal fraud is particularly insidious because it often hides in plain sight, buried under layers of legitimate transactions, making it hard to detect until it's too late.

External fraud schemes

Outsiders are no less dangerous, attacking with increasingly clever tactics that prey on the vulnerabilities of accounts payable systems. These external threats thrive on weak vendor verification processes and inadequate oversight, turning simple mistakes into significant financial hits.

Among the sea of fraud tactics, some are disturbingly common due to their simplicity and frequency:

- Billing schemes: Fake invoices from nonexistent vendors or for services never rendered, with payments intercepted by fraudsters.
- Check tampering: Forged endorsements, altered checks, or unauthorized checks funnel funds to illegitimate destinations.
- Expense reimbursement fraud: Employees inflate expense claims, adding personal costs or duplicating claims to fatten their wallets.
- Kickback schemes: Insiders conspire with outsiders, raking in fraudulent profits through over-invoicing.
- ACH fraud: Cybercriminals exploit sensitive banking information, initiating unauthorized transactions often after phishing attacks.

Understanding these schemes is the first step in crafting robust defenses. As these fraud tactics evolve, so too must the strategies to detect and prevent them, keeping organizations one step ahead in the battle against AP fraud.

As Brittany Carmichael points out,

"For our ACH vendors we do like a pre-note validation, and if you don't know what that is, that is like the penny-test payment to make sure that the bank accounts can receive the direct deposit payment from the clients."

The key red flags of accounts payable fraud

In the evolving landscape of accounts payable (AP) fraud, staying alert to the signs of foul play is crucial. Without robust internal controls and constant vigilance, fraudulent activities can slip through the cracks, costing companies dearly. Here are the red flags to watch out for:

Suspicious invoice details

Invoices that lack essential details, such as a vendor's address or contact number, should immediately raise red flags. Genuine invoices are typically comprehensive and detailed, so when critical information is missing, it could indicate an attempt to submit a fabricated bill.

Invoices that feature neatly rounded figures or unusually large payment amounts might be deliberately crafted to evade close scrutiny. These types of invoices often signal inflated charges designed to deceive and manipulate the payment process.

Another common fraud tactic is the repeated submission of invoices for the same goods or services. This method, aimed at securing multiple payments for a single transaction, exploits the repetition in processing to slip through unnoticed.

Questionable vendor information

If a vendor's contact details match those of an employee, it's a significant red flag, potentially indicating that the employee has created a fake vendor account to funnel money into their own pockets.

Vendors that use generic, free email services may lack the professionalism expected in legitimate business dealings, which should prompt a closer examination of their activities.

A sudden surge in payments to a specific vendor, especially without a corresponding increase in goods or services, suggests the possibility of an internal scheme within the AP department aimed at diverting company funds.

Duplicate invoices

Fraudsters often employ repetitive billing tactics, submitting the same invoice multiple times in hopes of securing multiple payments. This scheme frequently accompanies other forms of billing fraud, such as charging for non-existent services or products.

Implementing automated systems that match invoices with purchase orders and receipts is essential for detecting duplicate submissions. A rigorous review process for every invoice is crucial in minimizing the risk of unauthorized or erroneous payments.

Prevention strategies against accounts payable fraud

Accounts payable fraud isn't just a financial hiccup; it's a direct threat to your business's credibility and bottom line. To stay ahead of it, prevention needs to be more than a buzzword—it should be a core strategy. Start with airtight internal controls that leave no room for manipulation. Layer that with regular audits to catch discrepancies before they spiral. Automation technology is your next line of defense, minimizing human error and spotting red flags in real time. Finally, invest in your team with robust training that makes fraud prevention everyone's responsibility. The goal? Foster a culture where transparency is the norm, and vigilance is embedded in every process.

Strong internal controls

Strong internal controls are the backbone of a secure financial operation, setting the stage for vigilant oversight and a robust defense against fraud. At the heart of these controls lies the principle of segregation of duties—splitting responsibilities so no single individual can manipulate the entire process. This isn't just bureaucracy; it's a smart, strategic barrier against fraud. For example, the employee who processes payments should never be the one who authorizes them. By breaking up these roles, you create a system of checks and balances that's hard to game.

Multi-level approval processes further fortify this defense, adding another layer of scrutiny that catches anomalies before they become costly mistakes.

And don't underestimate the power of external audits. Regularly bringing in independent eyes keeps your financial reporting honest and transparent, ensuring that any weaknesses are spotted and addressed before they can be exploited. These measures collectively create a financial environment where security is ingrained, and fraud is far less likely to take root.

Bringing in fraud experts

Partnering with organizations that specialize in fraud prevention brings a level of expertise and focus that is crucial in today's complex threat landscape. These experts live and breathe fraud detection, staying ahead of the latest schemes and regulatory changes that might slip under the radar of in-house teams.

By working with dedicated fraud specialists, businesses gain access to cutting-edge tools and strategies that are continually refined to counter emerging threats. For instance, the Corcentric StopFraud solution brings together experts and technology that will run a 12-point validation solution for AP payments.

Joseph Griffith is a Corcentric StopFraud Validation Specialist who is clear on his responsibilities:

"My main priority or job function is to ensure information is accurate and legitimate, to verify company information with the main purpose of preventing any fraud attempts, making sure money is distributed correctly and appropriately from the client to the supplier without any wrongdoing involved."

This proactive approach doesn't just safeguard assets; it enhances the overall security posture of the organization, reducing vulnerabilities that could otherwise lead to significant financial and reputational damage.

Moreover, engaging with fraud experts provides a valuable perspective that goes beyond standard operational procedures. These professionals offer a comprehensive view of your risk landscape, identifying gaps in your current defenses and recommending tailored solutions that align with your business goals. The value of such partnerships lies not only in preventing fraud but also in fostering a culture of continuous improvement and vigilance. One key aspect is verbal validation. As Brittany Carmichael states,

"There's a risk involved in automating electronic payments and deposits. In terms of fraud prevention, you can only automate so much, but human intervention and human power is really where the protection comes from. For instance, taking the simple step to call a supplier and verify an email they just sent can catch potential fraud before it gets costly."

By working with AP fraud experts, you can shift from a reactive stance to a proactive, strategic approach to fraud mitigation, and free up your team to work on strategic tasks.

Regular auditing practices

Regular audits are more than just a box to check—they're your frontline defense against accounts payable fraud. They serve as an early warning system, catching irregularities before they morph into full-blown scandals.

To keep fraud at bay, regular reconciliation and review of accounts should be non-negotiable, paired with sharp-eyed audit procedures that leave no stone unturned. Though some may view audits as cumbersome, they're anything but. They are the bedrock of financial integrity, creating a culture of accountability that deters fraudulent behavior and ensures that your business remains vigilant and trustworthy.

Employing automation technologies

Automation in the accounts payable department transforms invoice processing from being labor-intensive and error-prone to a system characterized by efficiency and greater accuracy. Utilizing machine learning and AI-powered systems, these technologies can scrutinize extensive datasets quickly to detect anomalies indicative of fraud. For example, software can be set up to flag duplicate or false invoices, unusual patterns in vendor payments, or discrepancies in expense reports—all potential signs of fraudulent activity.

Automation also enhances record-keeping and generates an audit trail, considerably reducing the chance for payable fraud schemes to go unnoticed. Despite these advanced technologies, the human element remains a critical factor. As Joseph Griffith explains,

"So a lot of the validation process is automated, some with AI. When those systems trigger an exception, we do a manual intervention to validate say tax ID information, or bank information, as examples."

Sufficient oversight, combined with a continuous emphasis on ethical standards, ensures that automated systems function as intended and without creating new vulnerabilities. It is important to develop a strategy for when and where you use automation.

As Brittany explains,

"There is a risk involved with automating electronic payments and deposits. You can only automate so much, but human intervention and human power is really where the protection comes from."

Scaling with customer and supplier networks

In the battle against fraud, Accounts Payable (AP) professionals can find their strongest allies in the networks of suppliers and customers they cultivate. These networks don't just facilitate business—they become a vital defense system. Established relationships with known and reliable partners mean fewer surprises, and that familiarity translates into a much lower likelihood of dealing with fake invoices or deceptive practices.

Data sharing within these networks takes fraud prevention to another level. By pooling critical information like vendor payment histories, contract terms, and delivery confirmations, AP professionals gain the ability to cross-check invoices against real transactions effortlessly. As Joseph Griffith notes,

"We deal with multiple clients, so signing up with Corcentric and going through the StopFraud validation process makes it easier for suppliers and customers. An account change is updated across the whole network. So for instance, if a supplier needs to update their bank details, they only have to change this once with us, and we'll ensure the right bank information is used for every transaction with a customer in our network."

Strong supplier relationships, bolstered by these networks, allow for swift verification of any suspicious activity, ensuring that fraudulent claims are resolved before they cause financial harm. In essence, networks of suppliers and customers transform the AP landscape from one vulnerable to fraud into one that is secure and resilient.

Employee education and training programs

Educating company personnel on accounts payable fraud is a cornerstone of a robust protection strategy, transforming every employee into a frontline defender against potential threats. Comprehensive training should equip staff with the skills to identify red flags, such as fraudulent invoices and sophisticated billing schemes, including those involving fictitious vendors. By mastering the nuances of these schemes and learning how to accurately verify expense reimbursement requests, employees become adept at distinguishing legitimate transactions from fraudulent ones, thereby safeguarding the integrity of the payment process.

Regular, up-to-date training sessions are essential, ensuring that employees stay informed about the latest fraud tactics and the company's internal protocols for addressing suspicious activities. This ongoing education fosters a culture of compliance and vigilance, where prompt reporting and adherence to best practices become the norm. When every team member is aware and engaged, the opportunity for fraud to slip through the cracks is significantly reduced, creating an environment where integrity is not just expected, but ingrained in the company's operations.

Risk mitigation steps for organizations

To effectively mitigate the risk of accounts payable fraud, organizations need to establish a robust framework of internal controls, beginning with the segregation of duties and regular audits of AP processes. These foundational measures are critical in preventing unauthorized actions and ensuring that no single individual has control over all aspects of financial transactions, thereby maintaining the financial integrity of the organization. Beyond these basics, leveraging secure technology for transactions and conducting thorough vendor verifications are essential strategies to thwart common fraud schemes like business email compromise, where attackers impersonate legitimate vendors.

A meticulous approach to invoice review, especially when paired with cross-referencing related documentation, is another powerful defense against fraud. This practice can reveal inconsistencies or anomalies that often signal fraudulent activity. Moreover, integrating advanced technologies such as artificial intelligence and machine learning can enhance this process by enabling real-time detection of suspicious patterns in financial data, offering a proactive line of defense. Finally, continuous monitoring of payment processes, combined with ongoing employee education, ensures that the entire organization remains vigilant, significantly reducing the likelihood of fraud and reinforcing a culture of accountability and security.

Establishing a fraud response plan

An effective fraud response plan is integral to an organization's preparedness against accounts payable fraud. Cultivating a culture of awareness involves setting up clear procedures, offering fraud prevention training, and adopting AI-backed detection systems. Finance, IT, and accounts payable departments should work in concert with built-in checks and balances to ensure collective accountability.

Joseph Griffith provides one example where a supplier had their email hacked and didn't even realize:

"We had an instance where we had a request to update banking information. This needed to be done urgently as there was a very large payment about to be sent to the supplier. We received two emails in quick succession, each asking for the banking details to be updated, but the details were different in each case. In talking to the supplier, we realized that they had only sent the first email. Their email account had been hacked, but they only realized when we informed them."

Regular audits play a vital role in sealing gaps in control that could otherwise be exploited by

fraudsters. Automated accounts payable systems are not only efficient but also provide immediate transactional insights that can help pinpoint fraud. But what happens when fraud has been detected? You need to ensure you have a structured fraud response plan that can get to the root cause, solve the issue, and avoid similar fraud happening again.

Continuous monitoring and improvement

To take a proactive stance against fraud, organizations must prioritize continuous monitoring of financial transactions and implement regular audits. Advanced accounts payable software is a game-changer in this realm, offering real-time scrutiny and detailed reporting that are crucial for detecting anomalies and strengthening anti-fraud measures. This technology enables organizations to keep a constant watch on their financial activities, making it easier to spot irregularities before they escalate into significant threats.

AI-powered tools further elevate this approach by analyzing spending patterns at lightning speed, allowing for the rapid identification of fraudulent behavior and improving both preparedness and response times. Vigilance in vendor management, coupled with thorough due diligence, is essential for screening out bogus invoices and tracking vendor activity, which enhances the organization's fraud detection capabilities. Additionally, enforcing clear card-usage guidelines and regularly auditing card transactions are critical measures that help to identify and prevent fraudulent activities tied to card use.

Conclusion: *Fostering a culture of transparency, validation, and accountability*

Creating the right culture and processes are essential to safeguarding against accounts payable fraud. The foundation of a secure AP department lies in strong internal controls, such as segregating duties and conducting regular audits. These measures ensure that no single individual has unchecked control over financial processes, reducing the risk of fraudulent activity. Furthermore, educating employees on the risks and patterns of fraud, and the importance of integrity fosters an environment where ethical behavior is the norm, and vigilance is second nature.

Continuous oversight of financial transactions and thorough vetting of vendors provide an additional layer of protection against schemes like invoice fraud, billing scams, and the creation of fictitious vendors. Engaging external auditors introduces an impartial layer of scrutiny, promoting consistent compliance and reinforcing the organization's commitment to ethical practices.

Ultimately, when every level of the organization, from the AP department to senior management, is committed to understanding exposure and mitigating risk, this is the best way to protect the business. This collective vigilance not only prevents fraud but also sustains the company's integrity and long-term success.

Get *peace of mind.*

Web:

corcentric.com

Email:

info@corcentric.com

corcentric™

ABOUT CORCENTRIC

Corcentric is a leading global provider of best-in-class procurement and finance solutions. We offer a unique combination of technology and payment solutions complemented by robust advisory and managed services. Corcentric reduces stress and increases savings for procurement and finance business leaders by forming a strategic partnership to diagnose pain points and deliver tailor-made solutions for their unique challenges. For more than two decades, we've been a trusted partner who delivers proven results. To learn more, please **visit www.corcentric.com.**