Whitepaper

Mitigating AP Fraud Risk:

A CFO's Guide to Protecting Your Organisation

yooz

E-invoicing & P2P Automation. Easy. Powerful. Smart.

Content

The Most Common Types of AP Fraud 4

Red Flags: How to Spot AP Fraud Early 8

How Conventional Processes Leave AP Vulnerable to Fraud 12

Strategies for Mitigating the Risk of Fraud 15

Stop Fraudsters in their Tracks:
Future-Proof Your AP Department 19

Introduction

Every day, fraudsters are stealing millions of pounds from businesses just like yours. And they're getting better at it. From business email compromise (BEC) schemes and phony bank account change requests to fake invoices and phishing attacks, fraudsters are more sophisticated than ever – exploiting gaps in accounts payable (AP) processes faster than many finance teams can react.

Nearly 20 percent of AP leaders say their organisation experienced "considerably more" instances of attempted fraud in 2024 compared to 2023.[1]

No organisation is immune.

For CFOs, AP fraud isn't just a risk – it's an inevitability unless proactive measures are in place. A single fraudulent transaction can drain company funds, disrupt operations, and trigger regulatory scrutiny. Worse, falling victim to fraud signals weak financial governance, eroding investor confidence, damaging relationships with suppliers, and putting your credibility on the line.

CFOs and their teams are the last line of defence against AP fraud. It's the CFO's responsibility to safeguard corporate assets, ensure compliance with financial regulations, and mitigate risk before it leads to irreversible losses. Regulatory frameworks such as PCI-DSS and General Data Protection Regulation (GDPR) demand strict security controls. Failure to comply can result in massive penalties and legal exposure. A fraud incident can also shatter a company's reputation, making customers and stakeholders question whether their trust was misplaced.

Fraudsters aren't waiting. They are already targeting your organisation. They are using AI and social engineering to bypass traditional AP controls, slipping through outdated verification methods, and taking advantage of manual processes that leave AP teams vulnerable. A reactive approach is no longer enough. The only way to stay ahead of AP fraud is to take an aggressive, technology-driven stance – one that detects and prevents threats before they can drain your bottom line.

This guide will show you how.

1

The Most Common Types of AP Fraud

AP fraud takes many forms, but some tactics remain alarmingly effective.

BEC

BEC is among the most prevalent fraud schemes, where bad actors impersonate executives or suppliers to manipulate employees into authorising fraudulent payments. These scams often involve email spoofing, in which attackers create email addresses that closely resemble those of legitimate contacts, making them difficult to distinguish from authentic communications. Fraudsters also conduct extensive social engineering, gathering intelligence on an organisation's supplier relationships, approval processes, and payment cycles to craft highly convincing emails. To create a sense of urgency, these emails often demand immediate bank transfers, encouraging staff to bypass normal approval workflows.

More than two-thirds of AP departments experienced BEC scams in 2024.[2]

Phishing

Phishing schemes are another common attack method, using deceptive emails, text messages, or phone calls to trick employees into revealing sensitive information, such as login credentials or payment details. In credential harvesting attacks, staff unknowingly enter their login credentials into fraudulent websites that closely resemble legitimate portals. Once attackers gain access to an organisation's financial systems, they can manipulate transactions undetected. Fraudsters also send malicious email attachments disguised as invoices that contain hidden malware, compromising financial systems and exposing confidential data.

Fake invoices

Fake invoice fraud is a widespread tactic where fraudsters submit invoices for non-existent goods or services, exploiting weak verification processes. Some fraudsters create shell companies with fabricated business details and bank accounts, submitting fraudulent invoices that appear legitimate. Others manipulate legitimate invoices by altering payment details, redirecting funds to fraudulent accounts. In some cases, fraudsters engage in duplicate billing, submitting the same invoice multiple times to extract more payments.

Phony bank account change requests

Phony bank account change requests have become one of the most damaging forms of AP fraud. Fraudsters pose as legitimate suppliers and request that future payments be sent to a different bank account. These requests often appear urgent and credible, especially if they come from a spoofed email address or a fraudulent phone number that mimics the actual supplier's contact information. In some cases, attackers use deep-fake technology or AI-generated voice messages to imitate real supplier contacts, making the scam even harder to detect. Without a robust bank account verification process in place, organisations can unknowingly transfer funds to fraudulent bank accounts.

Supplier impersonation

Supplier-impersonation fraud is another significant risk, where fraudsters pose as legitimate suppliers and request changes to payment details, effectively rerouting payments to fraudulent accounts. They often use lookalike domains that closely resemble the official email addresses of legitimate suppliers, making it difficult for employees to detect fraud. Once trust is established, the fraudster submits a payment diversion request, asking the AP department to send future payments to a new, fraudulent bank account.

Nearly 70 percent of AP departments experienced attempted cheque fraud in 2024.[3]

Cheque fraud

Cheque fraud remains a persistent issue, even as organisations shift toward digital payments. Fraudsters use cheque washing techniques to chemically alter the details on stolen cheques, modifying payee names or amounts before cashing them. Others engage in forged signature schemes, where intercepted cheques are signed and cashed by unauthorised individuals. Criminals also engage in counterfeiting, producing fraudulent cheques that closely resemble authentic ones. Since paper cheques lack real-time fraud detection capabilities, organisations that continue using them remain vulnerable to these schemes.

Despite the shift towards digital payments, organisations that continue to rely on conventional invoice-to-pay processes and paper cheques are highly susceptible to fraud. AP teams must implement proactive measures to detect and prevent these threats before they result in financial losses.

2

Red Flags: How to Spot AP Fraud Early

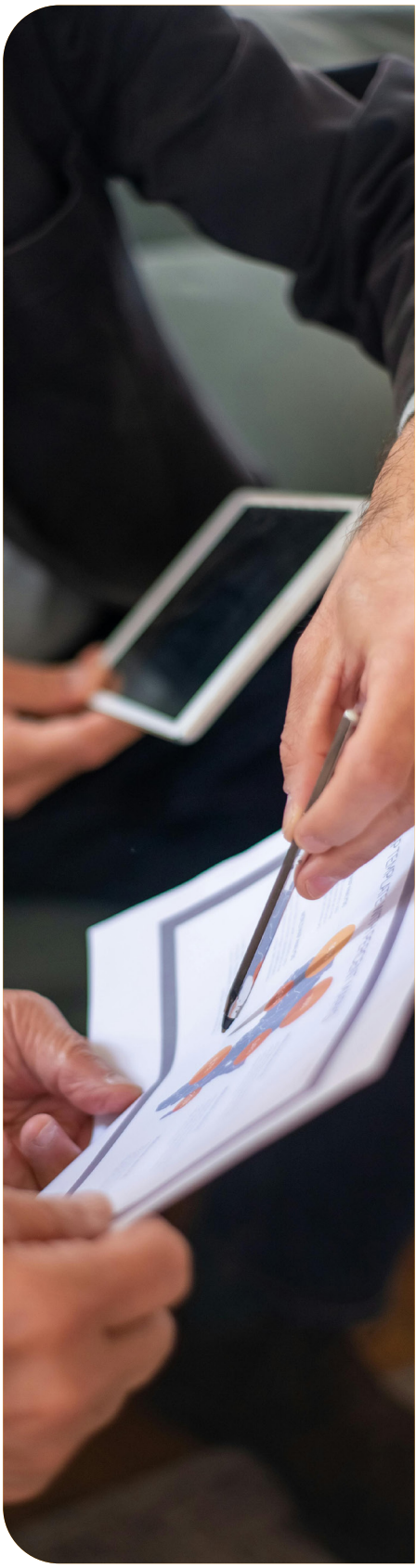
Fraud doesn't announce itself. It hides in plain sight, disguised as routine supplier requests, minor invoice discrepancies, and seemingly harmless payment changes. A single overlooked red flag – a rushed bank account update or an invoice just under an approval threshold – can be the difference between stopping fraud in its tracks and suffering a major financial loss. Fraudsters rely on AP teams being too busy to notice these warning signs, slipping fraudulent transactions through unnoticed.

But the patterns are there if you know where to look. Recognising and acting on these red flags early can mean the difference between business as usual and a crisis that threatens your bottom line.

A sudden and urgent request to change bank account details is one of the biggest red flags of potential AP fraud. Fraudsters often create a sense of urgency, claiming that failing to update the account immediately will result in service disruptions, shipment delays, or penalties. These high-pressure tactics are meant to push employees into skipping normal bank account verification steps.

A request that comes from a different email domain or personal email account should also raise suspicion. Fraudsters often use email addresses that closely resemble legitimate supplier addresses but contain slight misspellings or variations. Some may even switch to a generic email provider, such as Gmail, Yahoo, or Outlook, claiming that their corporate email is temporarily down.

Another red flag is a lack of supporting documentation to justify the change. Legitimate suppliers typically provide formal bank letters, voided cheques, or official communication confirming the request. If the request lacks these supporting materials or if the documentation appears altered, inconsistent, or of low-quality, it should be thoroughly vetted before any changes are made.



A phone number change along with the bank account update can also indicate fraud. Fraudsters may attempt to change the supplier's contact details to prevent verification calls from reaching the legitimate supplier. If a supplier suddenly provides a new phone number or insists on communicating only via email, AP teams should verify the request using previously known contact information.

Bank account details that differ from previous payment history should be scrutinised. If a long-term supplier suddenly requests payments to an unfamiliar bank, especially one in a different country or region, this could be a fraud attempt. Verifying the new bank details against official supplier records and confirming them with a known contact at the supplier organisation is essential.

Requests that contain grammatical errors or unusual phrasing can also be a sign of fraud. Many fraudulent emails contain awkward language, misspellings, or inconsistent formatting, especially if they originate from international fraudsters. If the tone or style of the request feels different from prior communications with the supplier, it should be investigated further.

Another critical red flag is an account name that does not match the supplier's legal business name. If the new account belongs to an individual or an unrelated business entity, it could indicate fraud.

Lastly, if the supplier does not respond to verification attempts using previously known contact details, this should be treated as a major warning sign. If an AP team reaches out to the supplier through its established phone number or email and does not receive a timely or coherent response, the request may be fraudulent. It is best to verify bank account changes with a trusted contact.

Beyond phony bank account change requests, there are other common red flags of AP fraud:

Unusual invoice amounts or payment frequencies.

Fraudsters frequently submit invoices that fall just below approval thresholds, allowing them to bypass additional scrutiny and review processes. An unexpected increase in payments to a particular supplier – especially for small, inconsistent amounts – may be a sign of a fraud scheme designed to avoid detection.

Duplicate or altered invoices.

Inconsistencies in invoice formatting, numbering, or supplier details may indicate that an invoice has been tampered with. Staff should carefully review invoices that contain slight variations, as fraudsters often make small, subtle changes to avoid detection. Additionally, multiple invoices with the same purchase order (PO) number should be flagged for review, as this may indicate an attempt to secure multiple payments.

Inconsistencies in cheque-payment records.

If an organisation notices an unusually high volume of cheque payments going to unfamiliar recipients or frequent cheque reissues, this could indicate fraudulent activity. Additionally, cheques that appear altered, feature mismatched signatures, or contain unusual formatting should be treated with suspicion.

Failing to recognise these red flags early can result in financial losses, operational disruptions, and reputational damage. By the time AP fraud is detected, the consequences can be devastating.

3

How Conventional Processes Leave AP Vulnerable to Fraud

Traditional AP processes expose organisations to significant fraud risks.

- **Manual data entry.** Manually keying invoice details is inherently prone to human error, increasing the likelihood of fraudulent invoices being processed without question. Since AP teams are often overburdened with high transaction volumes, they may lack the time or resources to verify each invoice manually, allowing fraudulent transactions to slip through.

Less than one-third of AP departments have software for automatically detecting fraudulent activity.[4]

- **Lack of real-time verification.** Many organisations do not have the capability to validate supplier details in real time, relying instead on outdated or inconsistent verification methods. Without automated verification, fraudulent suppliers can go undetected, and payments can be sent to unauthorised accounts. This gap is what fraudsters exploit, knowing that manual verification processes are slow, prone to human error, and often skipped under pressure.

- **Weak approval controls.** Paper-based approval processes can be easily manipulated, as fraudulent invoices can be manually inserted without a clear audit trail. BEC scams exploit weak internal communication channels, convincing employees to approve payments without verifying the legitimacy of requests. In a manual environment, the lack of segregation of duties and systematic workflows makes it easier for fraud to slip through unnoticed. Without automated controls, a single employee may have the authority to receive, approve, and process an invoice, increasing the risk of internal fraud or collusion. Additionally, under pressure to process payments quickly, staff may cut corners, bypassing verification steps or rubber-stamping approvals without proper due diligence. The absence of audit tracking further compounds the risk, making it difficult to trace fraudulent transactions, identify process breakdowns, or hold bad actors accountable. Without a clear, system-enforced record of who approved of what and when, fraud can go undetected until it's too late.

- **Email-based invoice submissions.** Fraudsters can intercept, manipulate, or fabricate invoices sent via email, making it difficult for AP teams to distinguish fraudulent documents from legitimate ones. Since traditional AP processes lack built-in authentication measures, fraudsters can exploit these vulnerabilities to gain unauthorised access to financial transactions. Email is not a secure channel – it lacks encryption and authentication protocols that verify the sender's identity, making it easy for fraudsters to impersonate suppliers or executives. Additionally, email does not provide chain of custody assurance, meaning there's no reliable way to track who accessed or altered an invoice at different stages. Unlike a centralised AP system, email doesn't log actions taken on an invoice, making it impossible to establish an audit trail or identify unauthorised changes. Email also lacks document retention controls, meaning invoices can be prematurely deleted, intentionally or unintentionally, with no way to recover them, potentially allowing AP fraud to go undetected.

Every day that organisations rely on outdated, manual invoice-to-pay processes, they leave the door wide open for AP fraud – without real-time verification, enforced approval controls, or secure document handling, it's only a matter of time before fraudulent transactions slip through.

4

Strategies for Mitigating the Risk of Fraud

Fraud prevention isn't about reacting after a loss. It's about putting intelligent, proactive defences in place before fraud occurs. As fraudsters develop more sophisticated tactics, finance teams must adopt a layered approach that combines automation, real-time detection, and strict internal controls.

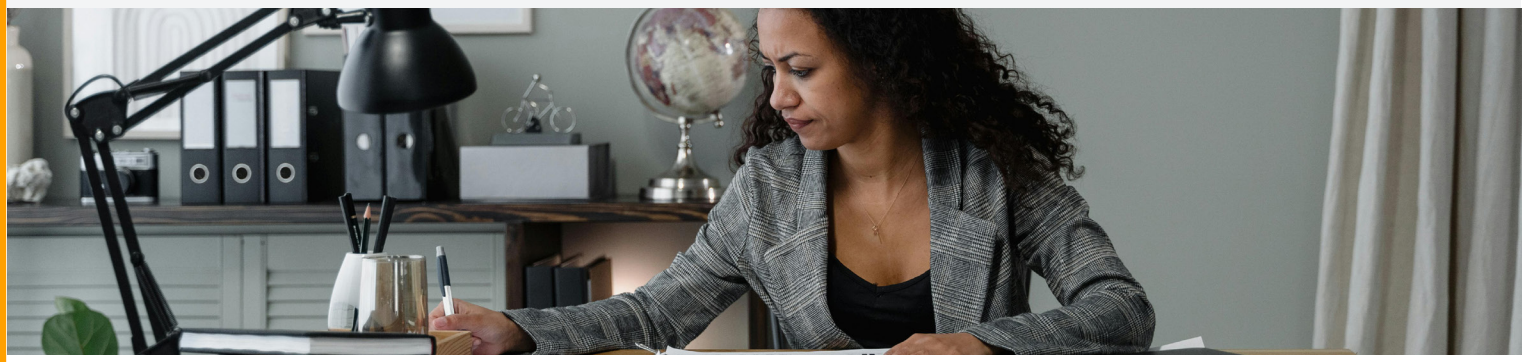
Below are key strategies to mitigate fraud risk in AP and ensure secure, compliant operations.

1 Use AI to identify fake documents.

Traditional fraud detection methods rely heavily on manual reviews, which are time-consuming, inconsistent, and prone to human error. AI-powered fraud detection changes the game by automatically scanning invoices and payment requests for anomalies. Deep learning and metadata analysis detect forged or manipulated invoices by examining document history, identifying hidden layers, and flagging any suspicious changes. For example, forensic analysis techniques such as steganography detection and PDF layer analysis can reveal whether an invoice has been altered – something that would be nearly impossible to spot with the human eye. By leveraging these advanced fraud detection methods, organisations can identify and block fraudulent invoices before they enter the approval workflow, significantly reducing the risk of unauthorised payments.

2 Automatically identify atypical payment behaviour.

Fraudsters often attempt to fly under the radar by submitting invoices with amounts that fall just below approval thresholds. Atypical amount detection technology can analyse historical transaction data and supplier payment patterns to flag any outliers. For example, statistical behavioural analysis – such as Z-score calculations – can identify invoices that deviate significantly from a supplier's normal billing patterns. If a supplier suddenly submits an invoice that is 30 percent higher than their usual charge, or if multiple lower value invoices appear suspiciously close together, the system can flag these transactions for further review. This real-time detection of abnormal payment activity helps organisations catch fraud early, before payments are processed.



3 Prevent phantom suppliers and supplier impersonation.

Supplier fraud is one of the most common and costly forms of AP fraud, often involving fake suppliers, supplier impersonation, or phony bank account change requests. Organisations can mitigate this risk with automated supplier authentication protocols that verify every supplier before payments are issued. An effective supplier authentication strategy includes real-time verification of supplier master data, ensuring that the supplier's legal name, banking details, and tax identification match official records. Automated checks can also detect inconsistencies in banking details, ensuring that the IBAN or account number on an invoice matches the approved supplier database. Any requested changes to supplier payment details should trigger alerts and require secondary verification, reducing the risk of fraudsters rerouting funds to unauthorised accounts.

4 Strengthen user access controls.

One of the biggest security vulnerabilities in AP fraud is unauthorised access to financial systems. Weak authentication methods – such as relying solely on usernames and passwords – can make it easy for fraudsters or insiders to manipulate invoices, change bank account details, or approve fraudulent payments. Implementing multi-factor authentication (MFA) and role-based access controls significantly strengthens security. MFA requires employees to verify their identity through multiple authentication methods before accessing AP systems, making it harder for cybercriminals to gain entry. Role-based access ensures that only authorised personnel can approve payments, change supplier details, or access sensitive financial data. Data encryption and HTTPS protocols further safeguard transactions, preventing unauthorised access to payment data.

5 Standardise workflows and segregation of duties.

Manual AP processes often lack systematic checks and balances, creating opportunities for fraud. A well-structured AP automation system enforces segregation of duties, ensuring that no single employee has end-to-end control over invoice processing and payments. Automated approval workflows introduce multi-level review processes, requiring invoices above a certain threshold to go through additional approval steps. This reduces the risk of fraudsters submitting high-value fraudulent invoices and ensures compliance with internal control policies. Parallel approval structures also allow multiple stakeholders to review high-risk transactions simultaneously, making it more difficult for fraudulent invoices to be processed without detection.

6 Improve tracking and control.

Fraud often goes undetected when there's no clear record of who approved what, when, and why. A robust fraud prevention strategy includes complete audit trails that track every action taken on an invoice – from submission to approval to payment. A detailed audit trail should link POs, invoices, and payment receipts, making it easy to trace any discrepancies. Additionally, real-time monitoring and alert systems can notify AP teams of any suspicious transactions, enabling them to respond quickly to potential fraud attempts. Comprehensive audit trails track every document action, ensuring compliance with leading financial security frameworks such as PCI-DSS, so finance teams always have a clear, traceable record of every transaction.

Fraud risk is constantly evolving, and manual processes alone can no longer keep up. By integrating AI-powered fraud detection, real-time anomaly monitoring, automated supplier authentication, strict access controls, workflow automation, and audit tracking, organisations can significantly reduce their exposure to financial fraud. A proactive approach to fraud prevention doesn't just protect company assets – it ensures compliance, strengthens supplier relationships, and reinforces financial integrity.

5

Stop Fraudsters in their Tracks: Future-Proof Your AP Department

The rising threat of AP fraud demands immediate action. Fraudsters are becoming more sophisticated, and the risks will only continue to grow. CFOs who take proactive steps today will not only protect their organisation's financial assets but also gain peace of mind knowing they have established a secure, fraud-resistant invoice-to-pay function. Implementing AP automation is the most effective way to eliminate fraud risks, enhance security, and ensure regulatory compliance.

This guide was created by Yooz, a leader in AI-powered AP automation.

With Yooz AP Automation, CFOs can take control of fraud prevention with an intelligent, automated solution that leverages AI, real-time monitoring, and built-in compliance controls to secure every step of the invoice-to-pay process. By eliminating manual risks, Yooz ensures finance teams can operate efficiently and confidently. Here are some of the fraud-mitigation capabilities that Yooz provides:

- **Smart Fake Detection.** Advanced AI and machine learning forensically analyse invoice metadata, detect anomalies, and flag suspicious invoices before they can be processed.
- **Atypical Amount Detection.** Statistical behaviour analysis identifies irregular supplier payment patterns, ensuring every transaction aligns with historical benchmarks.
- **Supplier Authentication and Management.** Real-time supplier detail verification, banking data identification, and Master Data enrichment help prevent fraudulent account setups.
- **User Authentication and Security.** Role-based access control, Single Sign-On (SSO), MFA, and AES-256 encryption ensure only authorised personnel can access sensitive financial data – preventing insider fraud and unauthorised access.
- **Process and Audit Assurance.** Comprehensive audit trails track every document action, ensuring compliance with leading financial security frameworks such as PCI-DSS, so finance teams always have a clear, traceable record of every transaction.

By combining cutting-edge AI, automated fraud detection, and robust controls, Yooz empowers AP teams to detect and prevent fraud – so CFOs can focus on business growth with confidence.

About Yooz

Yooz provides the smartest, most powerful and easiest-to-use cloud-based E-invoicing and Purchase-to-Pay (P2P) automation solution. It delivers unmatched savings, speed and security with affermable zero-risk subscriptions to more than 5,000 customers and 300,000 users worldwide.

Yooz's unique solution leverages Artificial Intelligence and RPA technologies to deliver an amazing level of automation with extreme simplicity, traceability and end-to-end customisable features. It simply integrates E-invoicing and AP Automation into information systems or ERPs with more than 250 native connectors, exceeding any other solution on the market.

Yooz is based in the US and Europe, with the UK Office located in London.

contact@uk.getyooz.com

+44 1252 741 536

yooz

E-invoicing & P2P Automation. Easy. Powerful. Smart.

To learn more about how Yooz can help you safeguard your AP process, visit **getyooz.com.**

1 IOFM, The State of Security and Fraud in AP in 2025

2 IOFM, The State of Security and Fraud in AP in 2025

3 IOFM, The State of Security and Fraud in AP in 2025

4 IOFM, The State of Security and Fraud in AP in 2025