Q4 2025 – Special Edition

Accounts Payable Fraud

Accounts Payable Departments are Targets for Fraud

Fraud is an ever-present threat for Accounts Payable (AP) departments. Unfortunately, the increasing sophistication of fraudsters has placed AP teams

squarely in their crosshairs. From phishing scams to invoice fraud, cybercriminals are constantly devising new ways to exploit vulnerabilities and redirect funds into their own pockets.

Why Accounts Payable Is a Prime Target

The Accounts Payable department handles large volumes of transactions, including payments to vendors, suppliers, and contractors. Since AP deals directly with money, it's a lucrative target for fraudsters. Common tactics used to exploit AP teams include impersonating vendors, submitting fake invoices, or manipulating payment instructions.

Fraud impacts a company's bottom line and can damage its reputation and vendor relationships. For AP professionals, understanding fraud risks and implementing preventative measures is crucial to avoiding costly mistakes.

Common Types of Fraud in Accounts Payable

- **Invoice Fraud:** Fraudsters create fake invoices that mimic real vendors, hoping AP teams will pay them without verifying authenticity. This scam often relies on urgency, pressuring AP staff to process the invoice quickly.
- **Vendor Impersonation (Business Email Compromise):** Cybercriminals pose as legitimate vendors or suppliers, often using email spoofing or hacked accounts to request payment or changes to bank details. AP teams may unwittingly send funds to fraudulent accounts.
- **Duplicate Payments:** Fraudsters exploit AP systems to submit invoices multiple times, hoping duplicates will slip through unnoticed. This can occur due to manual entry errors, weak controls, or poor visibility into payment history.
- **Payroll Diversion:** While typically aimed at HR departments, payroll diversion can also affect AP teams. Fraudsters send requests to update payment details for employees or contractors, redirecting funds to their own accounts.
- **Internal Fraud:** Fraud isn't always external. Rogue employees in the AP department may manipulate invoices, create fake vendor accounts, or approve payments to themselves. Lack of oversight and segregation of duties can enable internal fraud.

Red Flags of Possible Fraud

- **Urgent or rushed payment requests:** Fraudsters often use urgency to bypass standard checks.
- **Requests to change vendor payment details:** Always verify such changes independently and not through the same channel as requested (e.g., contact vendor directly and do NOT respond in the same manner requested).
- **Unfamiliar or suspicious invoices:** Cross-check invoices with purchase orders and vendor records.
- **Duplicate invoices:** Look for identical invoices submitted multiple times or slight variations in invoice numbers.
- **Emails with grammar errors or unusual tone:** These may signal phishing attempts or impersonation scams.

What to Do If Fraud Occurs

If you suspect fraud, act quickly to minimize damage:

1. **Freeze the transaction:** Stop payment immediately if the fraudulent request hasn't been processed yet.
2. **Inform your IT and Security teams:** They can investigate compromised accounts and block further access.
3. **Contact your financial institution:** Report the fraud to your financial institution to recover funds or prevent additional transfers.
4. **Notify management and legal counsel:** Keep leadership informed and consult legal teams for next steps.
5. **Improve processes:** Analyze how the fraud occurred and update policies to prevent future incidents.

Fraud is a constant risk for Accounts Payable departments, but vigilance and proactive measures can significantly reduce exposure. Remember, fraud prevention is not a one-time effort. It requires ongoing attention and adaptation to evolving tactics. If you're in Accounts Payable, beware of fraud and always verify before you pay.