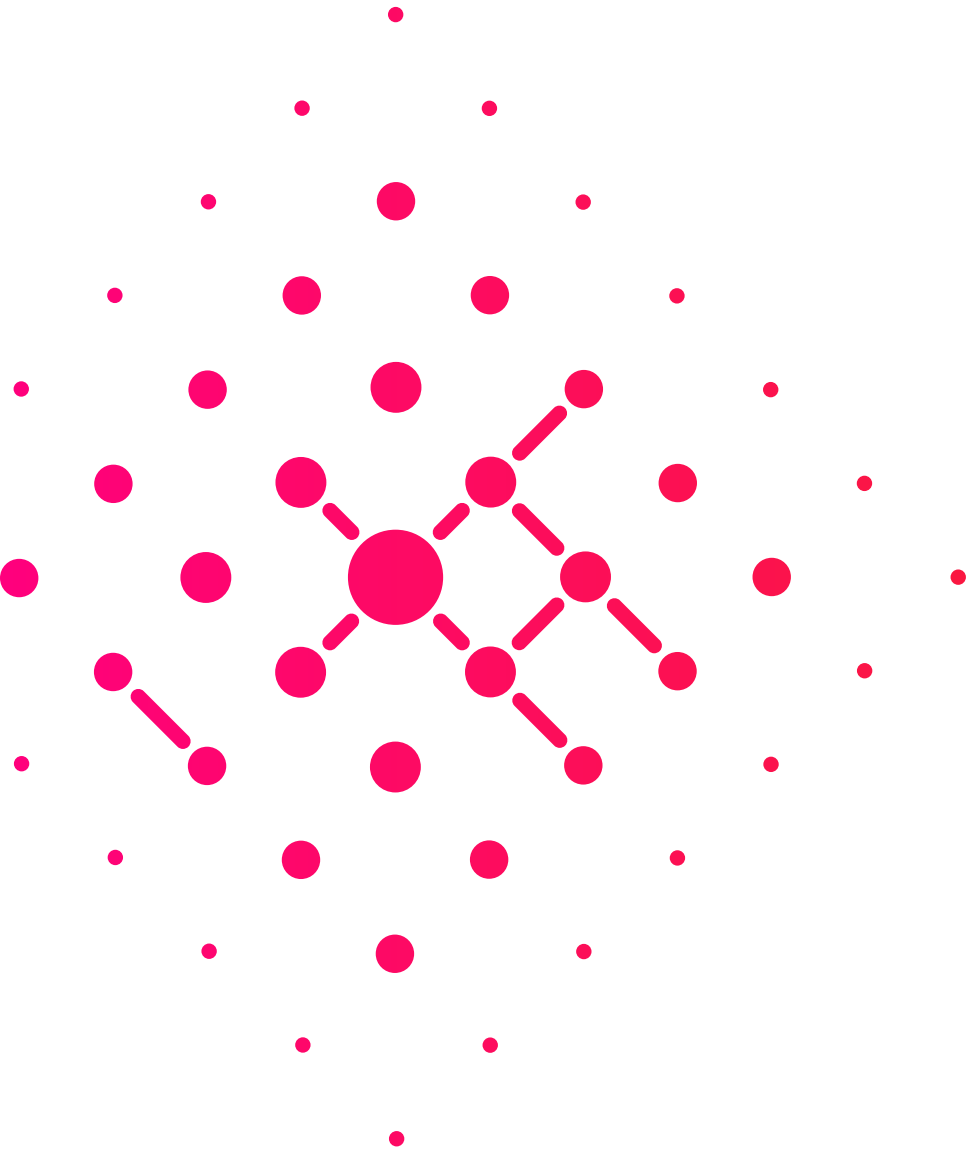
Edenred | Pay



The Ultimate Guide to Reducing Payment Fraud Risk

Businesses are under siege by bad actors determined to perpetrate payment fraud.

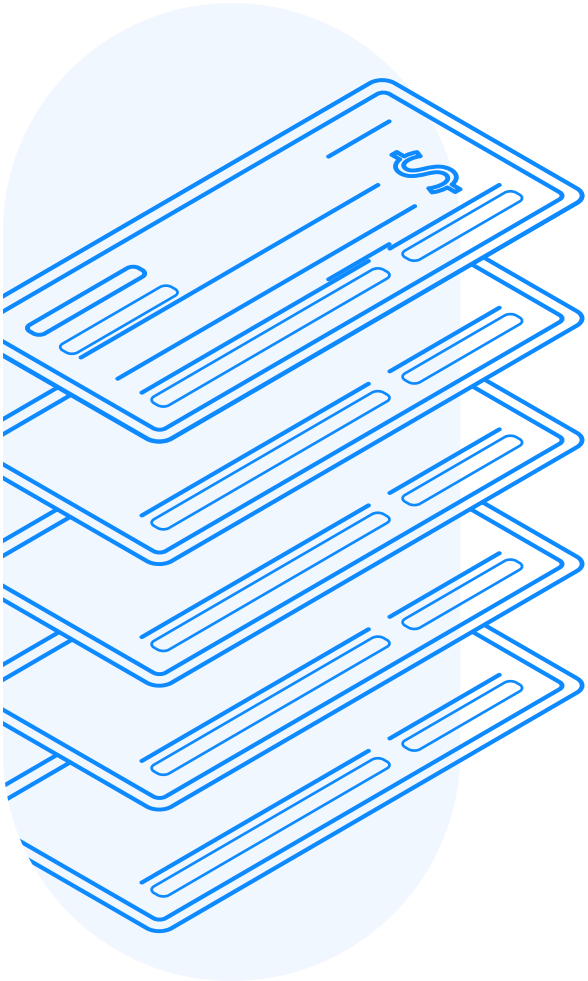
Businesses are under siege by bad actors determined to perpetrate payment fraud.

40% of departments experienced multiple instances of attempted or actual payment fraud.

58% of AP leaders surveyed by IOFM believe that their department is at higher risk of payment fraud compared to 3 years ago.

Left unchecked, payment fraud can result in big financial losses and significant reputational damage.

This white paper uncovers the latest check and digital payment fraud schemes, shares best practices for mitigating fraud risk, and reveals the signs that a banking change request may be fraudulent.



The high risk of check fraud

Fraud is inevitable wherever there are paper checks.

Half of the AP departments that detected a fraud attack in 2022 said it involved checks, per IOFM.

The root of the problem is that businesses have little control over paper checks once they drop them into the postal mail. Sophisticated networks of criminals are infiltrating U.S. post office distribution centers and using other means to steal checks sent through the mail. Once in possession of stolen checks, bad actors will alter the payee and deposit the check into a bank account that they control. In many cases, fraudsters will create phony businesses to facilitate the deposit of stolen checks. In fact, postal authorities and law enforcement agencies in many cities discourage against mailing checks.

Altered payees are only the tip of the iceberg when it comes to paper check fraud. Businesses also are falling victim to counterfeit checks, forged signatures, and fraudulent checks created using stolen or fabricated bank account details. Law enforcement officials have become so overwhelmed by the high number of check fraud cases that it's taking longer for victims to recover their stolen funds.

The bank details gleaned from stolen checks to establish new businesses or secure a line of credit. If businesses use paper checks to pay suppliers, they will be vulnerable to payment fraud.

Weaponizing email to commit fraud

The increased reliance on email to approve invoices for payment has created new fraud risks. Compared to invoice-to-pay solutions, email is not secure, it does not assure chain of custody, it does not enforce separation of duties or other policies, it does not log all actions taken on an invoice, and there's no stopping someone from deleting images ahead of the organization's retention schedule.

Importantly, bad actors are unleashing clever phishing schemes that exploit human weakness to gain access to financial systems and sensitive data.

69% of AP departments that detected a fraud attack in 2022 received a phishing scheme, IOFM says.

While it's tempting to think we'd never fall victim to phishing schemes, new technology and increasingly sophisticated tools for researching a company's trading partners and employees is putting businesses at greater risk.

Many fraudsters pose as a legitimate supplier or a trusted coworker, often a CFO or other member of senior management, requesting that the supplier's bank account details be changed to an account controlled by the bad actor. In many cases, the emails appear as long threads and incorporate the details that bad actors collected through social engineering or a successful phishing attack that provided them with access to the email of someone in the organization. In some cases, these emails come from an email address that appears nearly identical to that of a legitimate supplier or coworker.

Once funds have cleared a fraudster's bank account, they are hard to recover. Most fraudsters will close a bank account once an ill-gotten payment has cleared. And since ACH payments only take a few days to clear, the damage will be done by the time a supplier asks about a late payment. And it's easier than you might think for fraudsters to gain access to a trusted party's email.

One popular phishing scheme involves impersonating an express shipping company requesting the recipient click on a link to confirm delivery instructions. Another scheme uses spoofed emails from a tech company informing the recipient that they must urgently purchase additional storage space, or risk running out. Clicking on these links can provide fraudsters with the entree to perpetrate Business Email Compromise (BEC) attacks, account takeovers, and vendor impersonation schemes.

It's not just the actions of AP teams that can leave a business vulnerable to cyberattacks. Deficiencies in a supplier's security practices have a ripple effect on their customers.

Some fraudsters hack into vendor emails or business systems to learn information about the company, including its customers, open invoices, banking relationships, and payment preferences. Once the bad actor has the lay of the land, they take over the vendor's communications with its customers, eventually requesting bank account details be changed to an account they control. Fraudsters can learn enough about a vendor to create convincing emails to customers.

Increasingly sophisticated fraud schemes require businesses to beef up their fraud prevention.

Best practices for payment fraud mitigation

Corporate firewalls are not enough to prevent payment fraud. Bad actors can use phishing campaigns to expose internal systems, laptops, and sensitive financial data to the world.

Making matters worse, detecting phishing schemes isn't easy. Some fraudsters use hyperlinks contained within an email to get AP staff to unwittingly give up the source IP for a machine. And there's little stopping unsigned checks from falling into the wrong hands. The following best practices will help your organization mitigate its risk of fraud.

Educate your frontline staff.

Sixty-nine percent of AP department have implemented staff fraud training, per IOFM. Establish fraud prevention training for all new employees and a quarterly refresher for existing staff. Inform staff about the latest fraud schemes and how to detect them. Regularly review your training program and make updates as necessary. Urge staff to never click on a hyperlink from an untrusted source. Impress upon employees the importance of never downloading email attachments unless the sender is a trusted contact, and the file is expected. Remind staff to never provide their user credentials to anyone over the phone, even if the person they believe they are speaking with is a coworker. Instruct staff to never send user credentials via email, no matter who is requesting them. Require staff to lock their computer every time they step away. And ask staff to avoid using public Wi-Fi. Also consider having your IT department create simulated phishing schemes to test staff.

Validate invoice data.

Invoice-to-pay solutions compare the data extracted from invoices with purchase order (PO) and proof-of-delivery information residing in an ERP application or accounting software package. Unmatched invoices or invoices that require review – such as high-dollar transactions or invoices from new suppliers – are digitally routed to the appropriate individual based on pre-configured business rules. Comparing invoices to PO and proof-of-delivery information helps uncover inconsistencies that may indicate fraud. Additionally, reconciling invoices daily can help departments identify issues faster.

Improve visibility into invoice data.

When it comes to verifying invoice details, most AP departments are flying blind. Key data is not captured. Capture information is incorrect or incomplete. Data is not timely. Invoice information is poorly organized. And systems are fragmented. Invoice-to-pay solutions extract, validate, and centrally store all the invoice and header information from invoices. Authorized users can instantly access information, review audit information, and drill-down into archived data to uncover patterns. Capturing and validating complete invoice data helps identify potential fraud before initiating payment.

Enforce separation of duties.

Allowing one employee to approve invoices and payments is a recipe for disaster. Invoice-to-pay solutions build separation of duties into the platform. And audit logging of all actions taken on an invoice or payment provides accountability. Seventy-five percent of AP departments have employed segregation of duties, IOFM finds.

Beef up your procedures for banking change requests.

Sixty-three percent of AP departments have implemented programs for researching changes to vendor profiles, according to IOFM benchmarking data. Not every request to change a vendor profile or bank account details is fraudulent. But AP teams must be on the lookout for constantly evolving fraud schemes. Formalize your organization's policies for managing banking change requests. Ensure that staff understand and follow the steps for verifying bank account ownership. Compare supplier contacts, and any other details contained in a banking change request to information your organization has on file. Require multiple levels of verification for all bank account change requests, especially urgent ones. Require staff to double-check supplier details, whenever they are in doubt. Train staff on how to identify spoofed emails. Never rely solely on emails to confirm bank account change requests with suppliers. And consider using a third-party solutions provider to authenticate supplier banking details.

Pay suppliers with virtual cards.

Electronic payments significantly reduce an AP department's risk of payment fraud. Unlike paper checks, electronic payments cannot be intercepted and whitewashed. Suppliers always know when electronic payments will arrive, so they can act fast when delays occur. And the date that flows with electronic payments can be encrypted. Virtual cards offer several layers of protection that make them an especially secure way to pay suppliers. In fact, virtual cards are the most secure way to pay suppliers, according to data from the Association for Financial Professionals (AFP). Only 3 percent of all virtual card transactions experience attempted or actual fraud, AFP finds. Here's why. A virtual card can only be used once. A buyer can determine a payment amount or range, date range, and supplier for each virtual card. Unlike physical p-cards, virtual cards are plastic-less and cannot become lost or stolen. Approvals for virtual card payments also go through an organization's payable process, reducing the possibility of employee misuse. Suppliers only receive a portion of the 16-digit virtual card number, meaning there's no chance of a bad actor intercepting a card number. And leading payment solutions providers used advanced data encryption to protect virtual card information. The security mechanisms built into virtual cards may even convince suppliers leery of paying interchange fees to accept cards.

These measures will help mitigate your organization's risk of falling victim to payment fraud.

How to detect phony banking change requests

Fraudulent bank account change request schemes can be hard to detect and even harder to recover from. But there are clues in even the most convincing emails from fraudsters that things may not be as they appear. Here are some signs that a bank account change request may be fraudulent.

Email address anomalies. Fraudsters count on busy AP staff overlooking small changes to an email address the company has on file for a legitimate supplier (think: ".net" instead of ".com" or subtle changes to a URL). Reduce the possibility that your team will fall victim to a spoofed email address by scrutinizing the email address on bank account change requests.

Spelling errors, poor grammar, and awkward phrases. It is not uncommon for fraudulent banking change requests to originate outside the United States, with individuals who are not native English speakers. Spelling errors, inconsistent punctuation and capitalization, poor grammar, incorrect sentence construction, odd vocabulary choices and the use of wrong vernacular (e.g., "cheque" instead of "check" and a date that is not in U.S. format) can be tip-offs that a request merits close inspection. A sudden change in tone from your past email communications with a known contact for a supplier should also be a red flag.

Unknown individuals who are copied on an email. Phony bank account change requests sent by fraudsters will often copy individuals whose names they gathered through social engineering. The goal is to demonstrate the authenticity of the bank account change request (some emails even mention the person who is copied). Look closely at the email address of anyone copied on a bank account change request to ensure they are not a spoofed address.

Urgency. Haste can be a fraudster's best friend. When busy AP professionals rush to change bank account details, they are more likely to miss red flags or to circumvent key policies or procedures for verifying bank account ownership. That's why many bank account change requests pressure AP staff to make bank changes immediately. Thirty-six percent of AP departments that detected a fraud attack in 2022 said it involved a request for a rushed payment, according to IOFM benchmarking data. Remind staff that there are only a few instances when bank account details must be changed immediately. And a quick call to most suppliers will typically give buyers the time they need to verify account changes.

Wrong invoice details. Bad actors will sprinkle supplier and invoice details collected from phishing schemes to create convincing bank account change requests. As a result, invoice amounts, or invoice numbers may be from old payments or guesses based on past invoice patterns. Be sure to pay special attention to invoices with incorrect amounts or other details.

Document formatting issues. Many bad actors use templates to create their fraudulent requests to change bank account details. Take a hard look at bank account change requests for logos that appear skewed or off-center, poorly aligned text, and other irregularities. Also be sure to review the MICR line, supplier's logo, supplier's address, and bank logo on any copies of cancelled checks to ensure that the check hasn't been intercepted and doctored.

Scrutinizing bank account change requests will help your organization identify fraud attacks.

Mitigate your fraud risk

Payment fraud is rising, but the right technology and processes can help AP departments mitigate their risk. Educating front line staff, enforcing separation of duties, validating invoice information, enhancing AP visibility, beefing up procedures for validating banking change requests, and paying suppliers electronically are some of the ways that AP departments can stop fraudsters in their tracks.

Edenred | Pay