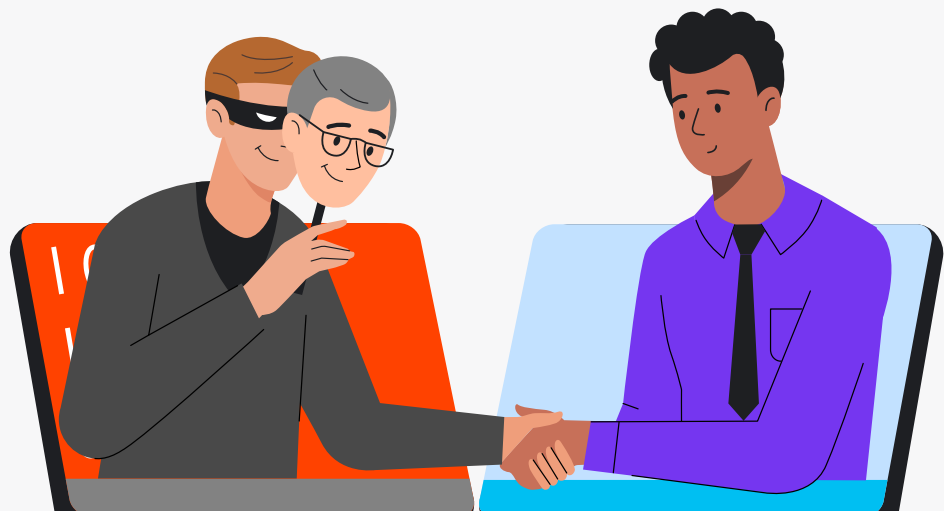


Stop Fraud Now: How to Protect Your Company with AP Automation

You may not have personally been victim to a financial scam or fraud but odds are someone you know has been. These days, criminals are getting even more sophisticated and outdated manual practices are an easy target for highly-skilled thieves to take off with your – or your company's – hard-earned cash.

Fraud is on the rise, with over 80% of organisations reporting being targets of an actual or attempted fraud attack, the second-highest percentage on record since 2009¹. No matter the size or strength of your business, all companies are vulnerable to scams and must actively protect against threats. Luckily, Quadient AP can help boost your defenses.

In this whitepaper, we'll explore how automation can protect you and your company from external and internal fraud within B2B payments. We'll also take a look at what contributes to inefficiencies within cross-border payments, and how you can make the process safer and more efficient.



External Fraud

Let's start with external fraud. Committed by vendors, or more likely fraudsters posing as vendors, this scam is designed to take advantage of vulnerabilities within company finance systems.

One big part of the problem is paper – traditional payment methods are risky as they don't provide the visibility that AP teams require to keep a business secure.

72% | **of businesses that made payments via paper checks experienced some kind of fraud in 2019¹.**

As more paper circulates, the perceived threat of fraud also increases. A report conducted by American Express found that there are 10 times more cases of fraud related to paper checks than Automated Clearing House (ACH) and wire transfers combined². The success rate of scams such as check forgery or Business Email Compromise (BEC) has been as high as 30% in the past³.

Case Study: Baltimore Accounting Blunder

In April 2019, an accounting clerk at the City of Baltimore received an email to route payments of an existing vendor to a new account. Without confirming the legitimacy of the email with the actual vendor, the clerk made the changes and put into motion a two-month-long scam that cost the City of Baltimore almost US\$62,337. What's more, the mistake was only uncovered when the real vendor submitted a complaint about the payment delay. The entire ordeal took nearly a year to unravel and almost as long to identify the culprit – all stemming from a single avoidable mistake.

² Companies Focus on Secure and Efficient Automated B2B Payment Solutions, Megan Doyle.

³ 2018 Survey Report: State of Treasury Fraud.

We know to avoid paper transactions, but fraud occurs frequently online as well. Here are some ways you can detect a BEC scam or other external fraud threats.

Signs of Fraud in Email and Domains



Invoices without vendor information such as an address or telephone number.



A purchase price that seems odd – could be too high or too low.



The vendor doesn't use a work email address and instead uses a free provider such as Gmail, Outlook or other.



Incorrect grammar or typos in the email.

Things You Can Do to Protect Against External Threats

To improve your AP security processes' resilience, you could set up a bank change form to initiate any changes within vendor banking details. When a vendor asks for their bank details to be changed, it should only be made after the vendor has accurately completed the bank change form. Additionally, you should:



Ask two or three questions to confirm the legitimacy of the request.



Confirm the banking change with the vendor.

Implementing walls of protection is key to keeping your finances safe, the problem is that it can be very time-consuming and difficult to manage.

How Nvoicepay Automation Protects Against Fraud and Threats

Quadient AP' partner and US-based payment automation company, Nvoicepay, helps track, update, and maintain payment data for their customers' suppliers. This means they are able to provide:



Outsourced Vendor Management:

By putting Nvoicepay in charge of collecting, updating and securing vendor payment data, they can help to mitigate any risk associated with storing this sensitive data in-house.



100% Payments Liability:

Every transaction is insured with a payment guarantee or warranty. Banks don't assume liability for fraud. Nvoicepay will indemnify 100% of vendor payments.



Dedicated support team:

A dedicated group of professionals is always standing by to help vendors process payments.

If you are looking to protect against external threats, Quadient AP has the solutions to guide you and your company through seamless AP payment security.

Internal Fraud

This type of fraud occurs when an internal party such as an employee or group of employees engages in misconduct such as submitting fake expenses or misusing company funds for personal gain. Unfortunately, even seemingly trustworthy company employees can wind up in sticky situations. In a recent survey, 34% of company respondents admit their corporate and commercial credit cards have been the target of fraud⁴.

43% | **of businesses are still managing expenses manually.¹**

If your company manages expenses manually small details can be missed or manipulated, causing unnecessary stress for not only AP teams, but the entire company.

Manual expense management also makes out-of-policy receipts much harder to catch – and when the volume of expense reports increases, so does the chance of fraud. There are too many opportunities for human error: duplicate invoices, spreadsheet inaccuracies, overlooked costs – simply being prepared can help put your company three steps ahead.

Case Study: Toner Sale Scam

Last year, an accountant at the Austin Public Library fraudulently purchased roughly US\$1.5 million in printer toner and then resold nearly all of the stock online. The employee also had access to 10 municipal credit cards, using them to buy nearly US\$18,000 in personal purchases, which the culprit executed through cash receipts and purchase approvals.

Things You Can Do to Strengthen Your AP Controls from Internal Threats



Document an expense policy and get it signed by employees.



Audit employee expenses regularly.



Conduct purchase order matching to streamline and control purchasing activity, while gaining visibility.

How Quadient AP Automation Protects Against Internal Threats

With Quadient AP automation, you can solve your expense management system and other AP challenges by:

- Setting up a multi-level approval matrix – this could be based on budget, department, entity and more.
- Using the Quadient AP App. Managers can approve invoices and employee expenses through the mobile app and ensure orders are being accurately filed. The app also allows employees to submit their receipts electronically.
- Allowing Quadient AP software to flag discrepancies such as duplicate invoices. This means you don't have to spend hours tracking down improperly filed invoices manually.

Internal threats are just as difficult to spot as external ones. Quadient AP automation takes away the hassle and ensures protection at every level.

Inefficiencies in Cross-Border Payments

Cross-border payments can be overly complex. When payments pass through multiple hands, it can be easy for things to get lost, mismanaged or overtaxed. In a survey we conducted in 2020, Quadient AP found that 71% of SMEs consider cross-border payments to be problematic⁷.

We also know a lot of vendors are moving away from paper checks. Part of the reason is the delay in receiving payments. Last year, 43% of invoices issued were still unpaid by their due date, an issue further aggravated by the COVID-19 pandemic⁸. Processes like paper checks not only cause delays and take a toll on the team – but they also affect corporate cash flow. Almost 15% of an organisation's annual operating budget is spent on maintaining outdated procedures⁹.

There are a number of factors that complicate international payments and open them up to fraud. One such challenge keeping records up-to-date with vendor information. In fact, 52% of businesses struggle with “inconsistent” vendor details¹⁰. It is not uncommon for data to be misfiled, lost or simply overlooked, resulting in missing or inaccurate information that can be vital for transactions. For this reason, 58% of finance leaders say better data insights could improve their regulatory compliance and help them identify fraud risks¹¹.

Case Study: Missing Verification at MacEwan University

In Edmonton, Canada, MacEwan University failed to verify an email from a vendor requesting a change in banking information in 2018. Tracing the fraudulent accounts to Montreal and Hong Kong, the perpetrators had used a cut-and-paste method to forge the actual vendor's logo into their fake email. MacEwan was defrauded of nearly US\$9.48 million. The final sum retrieved, which did not equal the amount stolen, took months to recover.

7 Implementing a Foreign Invoice Automation Solution, Cambridge, 2020.

8 Cash flows squeezed as USMCA feels the effect of COVID-19, Artadius, 2020.

9 Global B2B Payments Playbook, PYMNTS.com, 2020.

10 Challenges of Vendor Onboarding & Registration Survey, Endorinfo, 2020.

11 The CFO's Guide To Digitizing B2B Payments, PYMNTS.com, 2020.

Things You Can Do to Protect Your Company from Cross-Border Payment Inefficiencies

Implement a contact management and escalation procedure. Ensure that any changes can only be accepted by one person in the vendor organisation.

Set up a separate approval channel for payments and invoices. You could further customise this based on the amount or a specific vendor.

What Quadient AP Automated Payments Can Offer You



Validated data to reduce the risk of errors and exceptions. Verified and detailed data sets that are populated with all vital banking and company information to ensure safe and timely transactions.



The capability to accept a file from your accounting software or ERP. Seamless file sharing across all currency pairs, payment modalities and settlement accounts is standard with Quadient AP automation.



Flexibility in integration. Quadient AP systems work seamlessly with the most popular accounting software and offer the most relevant technology to fit any requirement.



Ability to mitigate foreign exchange risk. Risk management strategies implemented through Quadient AP automation are tailored to protect your budgeted rate and understand business objectives and risk tolerance.

Save Time, Cut Costs & Reduce Risk With AP Automation

Quadient Accounts Payable Automation by Beanworks is an essential all-in-one cloud-based accounts payable automation solution for the world's accounting teams. Our platform drives efficiency and productivity for busy AP teams. Quadient supports hundreds of thousands of customers worldwide in their quest to create relevant, personalised connections and achieve customer experience excellence.

Let's talk about automation.
Schedule a demo with an AP specialist:

beanworks.com/uk/demo-request/

