

# Guide:

## How to identify, detect, and control AP fraud

Uncover the key prevention measures for protecting your business from Accounts Payable fraud and ensuring long-term success.



### Quick links:

1. [Could accounts payable fraud happen in your business?](#)
2. [What is accounts payable fraud?](#)
3. [What are the common types of accounts payable fraud?](#)
4. [What are the common red flags that help identify accounts payable fraud?](#)
5. [7 tips for preventing AP fraud](#)
6. [Fraud detection and prevention with ApprovalMax](#)
7. [Fraud prevention checklist: 5 key improvement areas](#)

# Could accounts payable fraud happen in your business?

A business's reputation can be heavily damaged by fraud, which can result in significant financial losses. Not only could you lose the trust of customers and business partners, but you could also face serious legal consequences. In order to reduce the risk of fraud, you must have adequate internal controls, such as a fraud and corruption policy.

According to the **ACFE's Report on occupational fraud** (fraud committed by employees), a typical case of business fraud can go on for 12 months before it's detected and has an average price tag of \$117,000. External fraud can have even more staggering consequences and affect even the world's largest businesses.

In 2019, Facebook and Google lost over \$120,000,000 through a fraudulent business email scheme, after being deceived by a Lithuanian citizen pretending to be a company that both Facebook and Google did business with. In this instance, phishing emails were sent requesting funds to be transferred to the scammer's bank account.



**A typical case of occupational fraud can last 12 months before it's detected and can account for a loss of \$ 117,000**

This proves that businesses of all shapes and sizes are being targeted. In bigger companies, the fraudsters are counting on a high volume of transactions to bury the fraudulent transactions so they get passed through and go undetected. In regards to small businesses, it's usually assumed that they don't have the necessary resources or policies in place to detect fraudulent transactions in the first place.

## What is accounts payable fraud?

Any B2B payment made under false pretences falls into the category of **accounts payable fraud**. It can be committed by, or involve an organisation's staff, suppliers, or scammers. Accounts payable fraud, in essence, is performed by personnel with the right to execute payments. Such people can either be the offenders themselves, or victims of third parties who are very skillful in finding ways to get hold of your money.

The risk of becoming a victim of accounts payable fraud might seem daunting, considering the potential financial and reputational implications. But that's all the more reason to stop AP fraud before it actually happens. By raising awareness of the various types of fraud and having systems in place that help identify and thwart deception, you can protect the business and minimise any negative effects.

# What are the common types of accounts payable fraud?

Fraud can come in all shapes and sizes – it can be hard to spot and stop. Here's a brief overview of the most common types of accounts payable fraud to look out for.

## Internal fraud

Internal fraud, also known as occupational fraud, is performed intentionally by employees. According to the ACFE's report on occupational fraud, the most severe incidents are likely to occur in the accounting, sales, operations and executive management departments. Nearly half of reported cases were possible due to a lack of internal controls, or the ability to override existing controls. Unsurprisingly, 81% of the victim organisations in the report increased their anti-fraud controls afterwards, simply by strengthening their management review procedures and introducing proactive data-monitoring and analysis.



**Let's drill down into the most common internal AP fraud schemes.**

### 1. Billing schemes

A billing scheme is when an employee makes a payment to what looks like a legitimate recipient. In reality, the money is transferred to the employee's bank account; either directly or via a detour like a shell company.

A billing scheme can involve:

- Issuing false invoices for products or services that were never delivered.
- Colluding with a third party in "pass-through schemes" where a member of staff processes invoices through an account or company they control and gets a cut of the payment.
- Setting up a fake supplier account and generating false invoices which are then paid to the fraudulent employee.
- Issuing purchase orders and making payments for goods or services intended for personal use.
- Duplicating payments to suppliers and keeping what's later returned by them.

### 2. Kickback fraud

Kickback schemes are also known as corporate bribery – a supplier "pays" someone in the company (the buyer) to get preferential treatment when products or services are purchased. Kickbacks can be cash or gifts, or allow free use of a supplier's offering. Another variant is sharing the profits generated from inflated vendor invoices.



### 3. Reimbursement fraud

Expense reimbursement fraud can be committed by any employee that claims business expenses and is therefore not easy to spot. According to ACFE, it takes an average of two years before an organisation detects reimbursement fraud, which is usually based on:

- Mischaracterised expenses
- Exaggerated expenses
- Fictitious expenses
- Claiming the same expenses twice

### 4. Cheque fraud

Cheque tampering, meaning the physical forging of cheques, is one of the most lucrative AP fraud schemes. A clever and well-equipped person who knows all the steps involved in this type of fraud can go undetected for a long time. On the other hand, if caught, the paper trail created by cheque fraud serves as a trail of evidence for both the investigator and subsequent prosecution.

### 5. Automated Clearing House fraud

Automated clearing house fraud (ACH fraud) is on the rise, mainly because ACH transactions are often processed on the same day. There are various opportunities for personnel in accounts payable departments to engage in deception – by designating themselves as automatic bill payees, adding a new payee and sending money there, or transferring funds to a new account by using an already existing payee but altering the account information.

## External fraud

External fraud is committed by scammers, cybercriminals or suppliers. These are third party groups outside of an organisation.



### 1. Wire transfer scam

Wire scams occur quite frequently. The originators pose as someone you might know or pretend to be a respectable supplier, contact or other business you deal with. When you fall for it, they have you wire money directly into their account.

### 2. Phishing

Phishing attacks are typically carried out via email, but that's not the only way. You should be wary of suspicious phone calls, text messages, or malicious websites. Phishing attacks aim to trick you into thinking the message is from a reputable source, and these can vary in shape and form. **Here's a good overview of the most common phishing attacks to be aware of.**

### 3. Account takeover

Account takeovers are difficult to notice because they usually involve someone outside of the organisation who has access to your account, either through theft or stealing your login and password credentials. By taking over the account, the fraudsters are then able to execute fraudulent payments themselves, or lure others into doing so.

### 4. External ACH fraud

External ACH fraud is committed by external parties who gain access to the system via a compromised email account that's been targeted in a cyberattack. The criminals send invoices that appear to be coming from a known supplier, but when the attached file is opened or a bogus link is clicked, the attacker gets access to the system and is able to steal sensitive information.

## What are the common red flags that help identify accounts payable fraud?

Want to stay ahead of accounts payable fraud? Learn the common red flags to watch out for and protect your business from financial losses. Our expert-curated list includes signs like unusual suppliers, excessive payments, and incomplete documentation. Stay vigilant and safeguard your company's finances.

#### Red flags of AP fraud to watch out for:

- Suspicious or unapproved suppliers
- Unusual payment spikes to certain suppliers without corresponding increase in goods/services
- High payments to a single supplier
- Excessive spending on company credit cards
- Payments just below the approval limit
- Sequence or multiple split invoices
- Rounded invoice amounts
- Unprofessional or photocopied invoices
- Missing supplier details
- Suppliers using free email providers
- Supplier addresses matching employee addresses or resembling residential ones
- Excessive expenses on customer entertainment and gifts
- Incomplete or copied documentation
- Duplicate payments to the same supplier
- Abnormally low or high supplier prices
- Repeat purchases from suppliers with poor-quality goods/services
- Tips or complaints from employees, customers or suppliers.

# 7 tips for preventing AP fraud

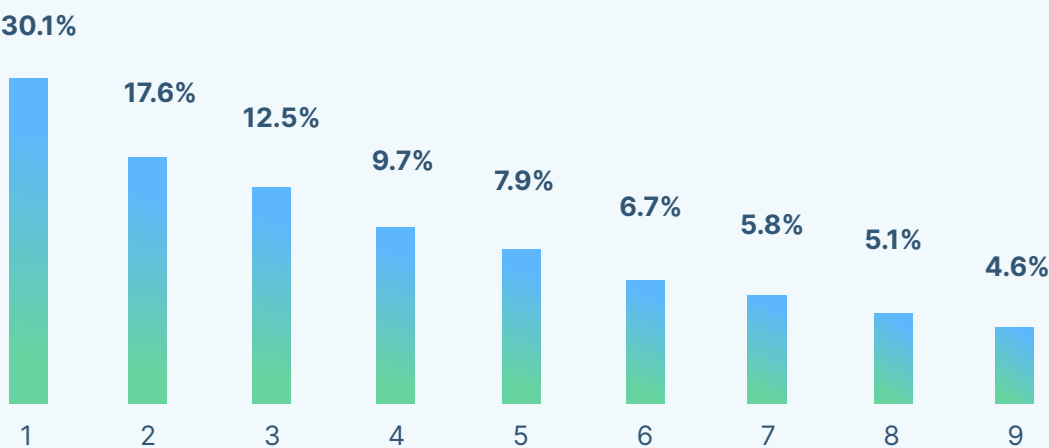
To stop fraud in its tracks, businesses must stay alert at all times and closely monitor their financial transactions for inconsistencies. Best practices include background checks on personnel, regular and unscheduled audits, clearly defined employee roles and responsibilities to separate financial duties, verifying vendors, and educating the staff. You can adopt the following strategies to prevent fraud from occurring in your business.

## 1. Be proactive

The only way to stay alert at all times is to be proactive. You need to perform regular audits and pay attention to any red flags on a daily basis. Running unscheduled audits can help identify fraudulent activities as well. Always check all transactions for the red flags listed above.


**Tip: apply Benford's law to check for inconsistencies in accounts payable.**

Benford's law, also known as the first-digit law, refers to the observation that in many real-life sets of numerical data, the leading digit is likely to be small. For instance, in about 30% of fraud cases the leading digit is 1 while it's only in less than 5 % the number 9. When deceitful staff members issue fictitious bills just below the approval amount, this proportion changes. And people who fabricate figures to commit external fraud tend to distribute their digits fairly uniformly. For instance, in the graph below, the leading digit is 1 in 30.1% of cases, while the number 9 only appears as the leading digit in 4.6% of cases.



## 2. Educate employees

Awareness training is not just about imparting knowledge on the various types of fraud. It should be geared towards providing practical information and teaching individuals how to recognise deception in their daily tasks. To ensure that the training is effective, it's important to use examples that closely mirror the responsibilities of your staff. By providing concrete case studies, employees can understand that even seemingly mundane tasks, such as matching invoices to purchase orders, serve a vital purpose and should be taken seriously.

 Make sure all training is relevant to your organisation and staff.

## 3. Set up a clear policy for expense reimbursement

A reimbursement policy must take into account your company's culture and budget, and specify the reimbursable expenses and how they are approved. This enables the accounts payable department and approvers to quickly determine whether an expense is reimbursable. A reimbursement policy should also set employee expectations around timing and what happens if a claim is rejected.

## 4. Segregate payment duties and authorities

To prevent fraud, you should operate your bookkeeping function and cheque accounts separately. By separating duties and authorities, you ensure that the same person is not in charge of both reviewing and paying invoices. Delegation of authority can involve quite complicated approval processes depending on the organisation's size and budget, especially for large amounts that require approval at all levels from a line manager to the CEO. Separating these responsibilities and implementing clearly delegated financial authority will significantly reduce risks over time.

## 6. Verify suppliers and vendors

Create proper procedures for approving all new suppliers before they're added to your company's database. This should be done by someone other than the person who enters new vendors into the system. To ensure that all suppliers are trustworthy, do a regular audit. Look for the warning signs mentioned earlier in this guide and physically check any dubious ones over the phone, online, or in person.

## 7. Automate the AP process to ensure security and segregation of authority

By automating the accounts payable processes, organisations can protect themselves against fraud, ensure segregation of duties, and adhere to purchasing policies. As automated approval workflows are based on set amounts and individual limits, employees can't overspend. With features like bill-to-purchase order matching and real-time audit trails, automation makes it easier for decision-makers to track all financial activity. In other words, automation impedes fraudulent activities and increases the odds of identifying it.

# Fraud detection and prevention with ApprovalMax

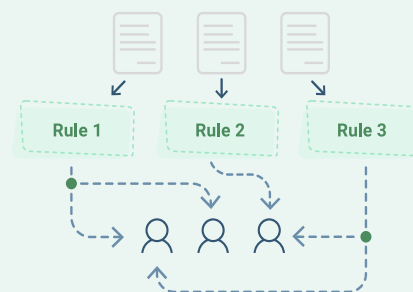
A business's reputation can be heavily damaged by fraud, which can result in significant financial losses. Not only could you lose trust with customers and business partners, but you could also face serious legal consequences. In order to reduce the risk of fraud, you must have adequate internal controls, such as a fraud and corruption policy.

**ApprovalMax** is an award-winning app that streamlines accounts payable and accounts receivable approvals. It prevents fraud by automating the segregation of duties and helps Xero users detect and avoid fraud. Let's look at how ApprovalMax helps to prevent fraud within your business.

## Flexible approval workflows to automate your delegation of authority policy

Delegated financial authority (DFA) is key to fraud protection, which is why you need to have a policy that defines approval limits, and appropriate individuals in the decision making process.

ApprovalMax lets you implement your DFA policy in an easy and safe manner. You can set up approval rules to be as simple or as complex as you need. It's also faster than manual approvals. 50% of bills in ApprovalMax are approved in less than 1 day, and 25% within 2 days.



## Audit trail and audit reports

Fraud attempts are a lot less likely to occur when individuals know that their activities are traced and recorded.



ApprovalMax generates a detailed audit report for each approved document, which is published in Xero, as well as an audit trail that's available in the app itself. In addition, you can grant auditors read-only access to all approval workflows so that they can view and analyse your approval process and suggest further fraud protection improvements.



## Restricting access to Xero

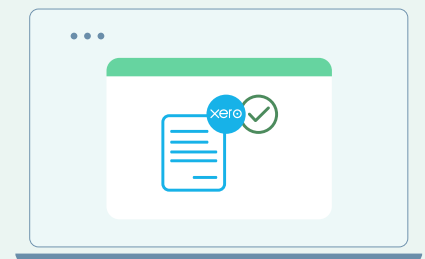
The majority of financial fraud occurs when people are able to change crucial data without being noticed. Although you can submit financial documents for approval in Xero, this means giving approvers access to Xero; however, it's impossible to restrict what they can see and do in Xero.



In ApprovalMax, decision-makers only ever see the information relevant to the documents they are approving and don't need access to the general ledger.

## Detecting changes after approval and documents approved directly in Xero

Even when you have a delegation of authority policy implemented in ApprovalMax, there's still the risk of documents being approved directly in Xero, or getting changed after the approval process in ApprovalMax has been completed.



To keep track of this, ApprovalMax has two special features: "Fraud detection – bypassing the approval workflow" and "Fraud detection – changes after approval". When they are activated, the organisation's administrator will be notified about all documents approved directly in Xero and any changes made to approved documents (you can specify which changes are to trigger such notifications, e.g. a changed amount, contact, account, tracking category, item or description).

## Matching bills to purchase orders

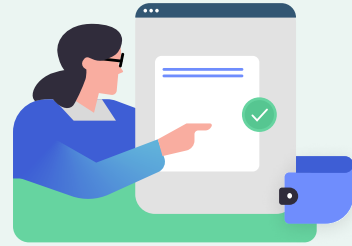
Matching bills and purchase orders ensures accuracy of payments.



In ApprovalMax, if the total amount of all bills linked to a purchase order exceeds its original amount, bill approval will be blocked. Once blocked, bills and purchase orders can only be authorised once they have been matched correctly, or the issue has been fixed. You can also attach a delivery note or proof of acceptance (either an acceptance certificate or photos of the delivered goods) to any document, then match bills and purchase orders to proof of delivery.

## Supplier approvals

When anyone can order anything from any supplier, there is a risk of supplier fraud. To strengthen controls, implement automation to ensure purchase orders are only raised with authorised suppliers.



ApprovalMax features include a supplier approval workflow as well as the option to limit which suppliers are available each purchase order requester. The contact (supplier) approval workflow ensures that new vendor's are vetted by decision-makers because an order can be placed with them. With approval automation, you can't miss a step or (un)intentionally change the predefined procedure.

## Bill duplicate detection

ApprovalMax cross-checks attributes on bills such as supplier, data and amount to catch any potential duplicate documents. If two bills appear to be duplicates, ApprovalMax instantly notifies approvers so they can be checked then approved or rejected. This functionality helps to prevent duplicate payments.



## 2FA and auto-logout

To safeguard the account information, you can use 2-factor authentication in ApprovalMax. Furthermore, if a user has been inactive for more than 15 minutes, ApprovalMax will automatically log them out.



# Fraud prevention checklist:

It's time to put a few things in action to prevent your business from fraud.

Use this checklist to get started.

## 1. Educate employees

Hold mandatory training for all employees to explain how AP fraud can affect your business and what they can do to prevent it

Include industry-specific examples of fraud that are relevant to your organisation

Set up recurring training regularly and update the training content as new fraud methods come up

## 2. Segregate tasks and approvers

Split up the reviewing of invoices and the payment process so that each task has to be done by two different people

Create a delegated financial authority (DFA) matrix to clearly define approvers in your business and the limits that they can approve

## 3. Watch out for the red flags

Make the red flags list a part of your security training and distribute it as a memo for the AP team

## 4. Verify your vendors and suppliers

Create a process for new vendor verification and split up the roles for reviewing vendors, and then accepting them into your system. Ensure there are two different people across these roles, one person entering new contacts to the system, and the other person verifying them

Create a delegated financial authority (DFA) matrix to clearly define approvers in your business and the limits that they can approve

## 5. Start using ApprovalMax

Start a 14-day free trial of ApprovalMax to reduce the risk of fraudulent activity.