GUIDE · FRAUD CONTROL

How to identify, detect, and control AP fraud.

A working playbook for finance leaders — uncover the prevention measures that protect your business from accounts payable fraud, and build the controls that survive audit, scale, and turnover.

THE AP LIFECYCLE · WHERE APPROVALMAX OPERATES

FOUR STAGES · ONE CONTINUOUS CONTROL

Capture

OCR & intelligent capture — invoices and expenses enter clean.

Approve

Automated routing with policy enforced and a record created.

Catch risk

Anomaly detection at approval — systematic safeguards, not intentions.

Pay & complete

Defensible audit trail and clean GL sync end the cycle.

WRITTEN FOR

CFOs, finance directors, and controllers responsible for spend governance — and the AP teams who execute it daily.

13 PAGES

CONTENTS

What you'll find in this guide.

Seven sections, structured around how fraud actually moves through an organisation — from where it hides, to how to detect it, to the operational controls that stop it before it lands.

WHY THIS MATTERS

Every dollar that leaves the business should leave with your permission.

Fraud rarely arrives as a single event — it lives in the gaps between processes, in the absence of segregation, in the workflow no one re-read. This guide is for the people responsible for closing those gaps before they cost the business its capital, its trust, or its audit.

SECTION 01

Could AP fraud happen in your business?

If your reputation, your audit trail, and your capital base depend on the integrity of payments leaving the business, then the answer is the same answer the ACFE has reached every year — yes, and you'd want to know early. Here's the shape of the problem.

12 months

average time to detect a typical occupational fraud case

Twelve months of fictitious invoices, duplicated payments, or quietly inflated claims — all running through a system that, on paper, was working. The median case carries a price tag of **$145,000**, with average losses reaching **$1.7M** per case — and the trust costs are harder to put a number on.

SOURCE: ACFE — OCCUPATIONAL FRAUD 2024: A REPORT TO THE NATIONS

Businesses of every size are targeted. In larger organisations, fraudsters rely on transaction volume to bury anomalies. In smaller ones, they assume the controls aren't there to catch them in the first place. Both assumptions are reasonable — and both are correctable.

EXTERNAL FRAUD · REAL EXAMPLE

Facebook and Google · $120M lost to a single phishing scheme

A Lithuanian national posed as a hardware vendor both companies legitimately did business with, sent fraudulent invoices over email, and routed funds to accounts he controlled. The scheme ran for two years. The defence wasn't a better firewall — it was an approval workflow that asked the question "did we really order this?"

SECTION 02

What is accounts payable fraud?

Any B2B payment made under false pretences. It can be committed by staff, by suppliers, or by external scammers — but in every case, it requires someone with the right (or stolen access) to execute a payment. There are two families of risk.

INTERNAL · OCCUPATIONAL

Fraud committed inside the organisation

Performed by employees with payment authority — most often in accounting, sales, operations, or executive management. Nearly half of reported cases trace back to a missing internal control, or the ability to override one that existed.

82% of victim organisations strengthened their controls afterwards. The fix is rarely complicated — it's just non-negotiable.

EXTERNAL · THIRD-PARTY

Fraud committed against the organisation

Executed by scammers, cyber-criminals, or compromised suppliers. The vector is almost always the same — a payment instruction that looks legitimate, sent through a channel that wasn't designed to verify.

$120M lost in a single business email compromise scheme — the largest publicly disclosed AP-fraud loss to date.

In bigger companies, fraudsters count on transaction volume to bury fraudulent items. In smaller ones, they assume the policies and the segregation of duties aren't there to catch them. Both assumptions get tested every quarter.

SECTION 03 · INTERNAL

Five schemes that hide in plain sight.

The most common internal AP fraud patterns — what they look like, who they target, and the operational gap each one exploits.

BILLING SCHEME 01

Payments to a "legitimate" recipient that's actually you

An employee makes a payment that looks routine. The money lands in their own account — directly, or via a shell company designed to launder the trail.

- False invoices for services that were never delivered
- Fake supplier accounts paid against fabricated invoices
- Duplicate payments, with the refund pocketed
- Pass-through schemes via a controlled third party
- Purchase orders raised for personal-use goods
- Round-amount invoices designed to clear without scrutiny

KICKBACK FRAUD 02

Corporate bribery, dressed as preferred-vendor terms

A supplier "pays" the buyer — cash, gifts, free use of services, or a cut of inflated invoice profits — in exchange for preferential treatment.

REIMBURSEMENT FRAUD 03

Mischaracterised, exaggerated, or duplicated claims

The hardest scheme to spot — anyone who claims expenses can run it. ACFE reports an average of two years to detection. Watch for fictitious receipts and the same charge claimed twice.

CHEQUE TAMPERING 04

Physical forgery — lucrative, traceable, slow to catch

One of the most lucrative schemes when it works. The paper trail eventually becomes evidence — but only after the loss has already landed and accumulated.

ACH FRAUD (INTERNAL) 05

Same-day rails, same-day damage

Personnel designate themselves as auto-payees, add new payees mid-cycle, or alter account information on existing suppliers. ACH's same-day settlement makes recovery rare.

SECTION 04 · EXTERNAL

Four schemes from the outside.

External fraud almost always rides on a moment of trust — a familiar supplier name, a routine payment cadence, an inbox that didn't ask the second question.

WIRE TRANSFER SCAM 01

"Update our payment details — urgent"

The originator poses as a known supplier, contact, or business you deal with. The instruction is plausible, the timing is convenient, and the wire is irreversible.

PHISHING 02

Email is the most common vector — but not the only one

Phone calls, SMS, malicious websites, and lookalike domains all qualify. The ask is always the same — share credentials, click the link, or wire the funds.

ACCOUNT TAKEOVER 03

Stolen credentials, executed payments, no alarm

Hardest external attack to detect — the fraudster operates inside a real account. They execute payments themselves or lure colleagues into approving payments that look internally generated.

EXTERNAL ACH FRAUD 04

Compromised supplier inboxes, weaponised invoices

The criminal gains access to a real supplier's email, then sends invoices that arrive from the right domain. The attached file or link delivers the payload — and the access compounds.

THE PATTERN THAT TIES THEM TOGETHER

Trust without verification is the attack surface.

Every external scheme above succeeds because someone, somewhere, accepted a payment instruction at face value. The technical defences matter — but the procedural defence is what catches it: a workflow that requires an out-of-band check before a new account, a new amount, or a new supplier ever processes a payment.

SECTION 05

17 red flags to watch for.

Print this sheet. Distribute it as a one-page reference for everyone in the AP function. None of these signals are conclusive on their own — but two or three appearing together is reason to stop the workflow and verify.

AP fraud red flags · operator reference

17 signals

01 Suspicious or unapproved suppliers in the ledger

02 Unusual payment spikes to a supplier without matching activity

03 High concentration of payments to a single supplier

04 Excessive spending on company credit cards

05 Payments structured just below the approval limit

06 Sequence or multiple-split invoices from one vendor

07 Rounded invoice amounts ($1,000 / $5,000 / $10,000)

08 Unprofessional or photocopied invoices

09 Missing supplier details — no VAT/EIN, no address, no phone

10 Suppliers using free email providers for invoicing

11 Supplier addresses matching employee or residential addresses

12 Excessive customer entertainment or gifts on expense reports

13 Incomplete, copied, or photocopied documentation

14 Duplicate payments to the same supplier

15 Abnormally low or high prices versus market

16 Repeat purchases from suppliers with poor-quality goods

17 Tips or complaints from employees, customers, or other suppliers

· *Two or more flags together — escalate before approving.*

SECTION 06

7 tips for preventing AP fraud.

Background checks, unscheduled audits, defined roles, vendor verification, and education — the operational basics, in the order they earn their keep.

01

Be proactive — audit on a cadence, and audit unannounced

The only way to stay alert is to be proactive. Run regular audits, run unscheduled ones, and check every transaction against the red-flag list on page 07. The schemes that hide are the ones no one's looking for.

02

Educate employees with examples that mirror their work

Awareness training only works if the case studies look like the AP team's actual desk. Use real-shape examples — invoice matching, vendor onboarding, expense reviews. Refresh annually as new methods emerge.

03

Set a clear policy for expense reimbursement

Define what's reimbursable, who approves it, and the timeline for resolution. The AP function and approvers should be able to clear or reject a claim without ambiguity. Ambiguity is where reimbursement fraud lives.

04

Segregate payment duties and approval authorities

Operate bookkeeping and cheque accounts separately. The same person should never review and pay the same invoice. Build delegated financial authority (DFA) into the workflow itself, not just the policy document.

05

Apply Benford's law against suspicious data sets

Real-world numerical distributions favour leading digit 1 (~30%) over 9 (~5%). When fabricated invoices cluster just below approval limits, the curve breaks. See p. 09 for the full picture.

06

Verify suppliers before they enter the database

New-vendor approval should be a separate step performed by a separate person. Audit the supplier list regularly — physically verify any dubious entries by phone or in person before the next payment runs.

07

Automate the AP process — security and segregation by default

Automated approval workflows enforce limits, enforce segregation, and produce the audit trail by themselves. Bill-to-PO matching catches the duplicates. The fraudster's biggest ally is a manual process — remove it.

SECTION 07 · DETECTION TECHNIQUE

A test you can run on Monday morning.

In genuine numerical data — real invoice amounts, real expense reports — the leading digit follows a predictable distribution. **Benford's law** says the digit "1" leads ~30% of the time, while "9" leads under 5%. Fabricated figures don't follow it.

REAL DATA · DIGIT 1 LEADS

30.1%

of invoices in genuine data sets

REAL DATA · DIGIT 9 LEADS

4.6%

of invoices in genuine data sets

WHERE IT BREAKS

When staff issue invoices clustered just below an approval threshold (say, $4,800 instead of escalating to a $5,000 approver), the leading-digit distribution flattens — too many 4s, too few 1s.

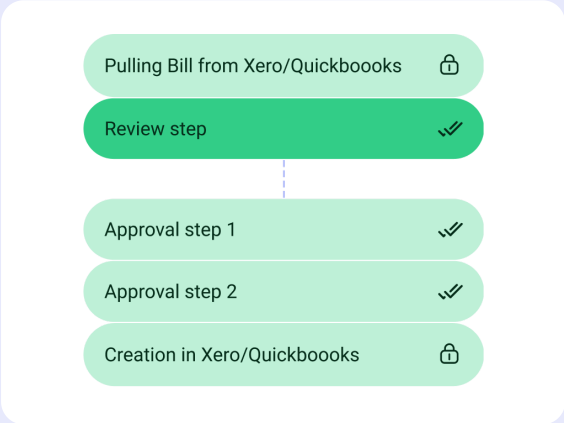
HOW TO USE IT

Run the test against any large numerical data set: invoice amounts, expense claims, PO values. Compare the distribution to Benford's. A meaningful divergence is not proof of fraud — but it is sufficient cause to investigate.

SECTION 08

How ApprovalMax closes the gaps.

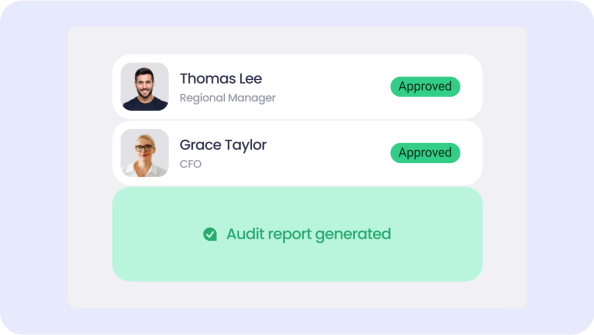
An award-winning approval automation app for Xero, QuickBooks Online, and NetSuite — built specifically to automate segregation of duties and produce the audit trail that surfaces fraud before payment.



Flexible approval workflows that automate your DFA policy

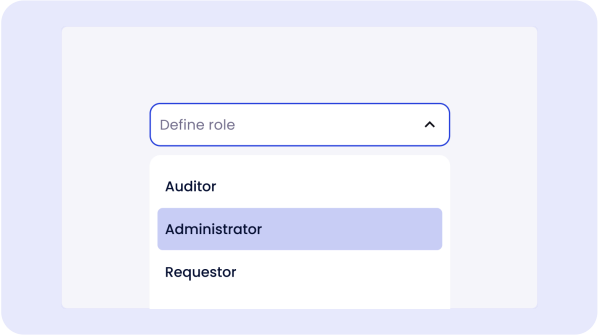
Set up rules as simple or as complex as the business needs — multi-step, multi-approver, threshold-driven, role-driven. Faster than manual approvals; the workflow is the policy, not a separate document.

50% OF BILLS APPROVED WITHIN 1 DAY · 25% WITHIN 2 DAYS



Audit trail and audit reports — published to your accounting system

Every approved document carries a detailed audit report into Xero / QBO / NetSuite, plus a full activity log inside ApprovalMax. Auditors get read-only access. Activity that's traced is activity that doesn't happen.



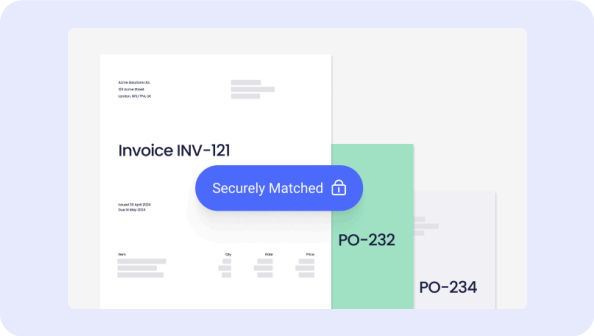
Restricted ledger access — approvers see only what they need

Most fraud occurs when people can change crucial data without being noticed. In ApprovalMax, decision-makers see only the documents they're approving — never the general ledger.

SECTION 09

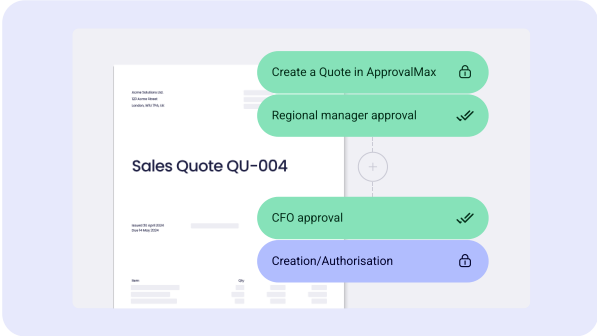
Controls that catch what approvals alone won't.

Even with a sound delegation-of-authority policy, fraud can still slip through — documents approved directly in the ledger, amounts changed after the fact, duplicates issued under different invoice numbers. Four ApprovalMax features address each of these specifically.



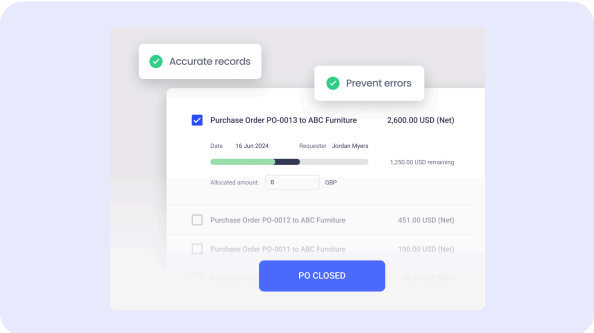
Bill-to-PO matching · accuracy of payments

If the total of all bills linked to a PO exceeds its original amount, approval is blocked until matched correctly. Attach delivery notes or proof of acceptance, then match bills against proof of delivery.



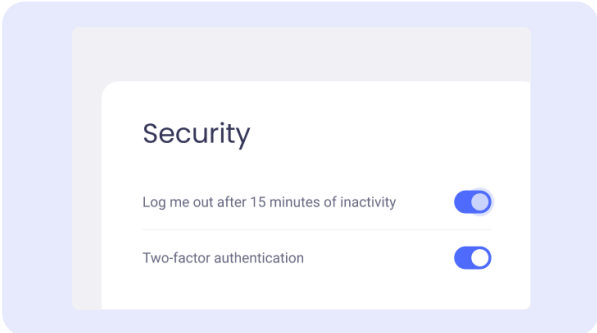
Supplier approval workflows · vetted contacts only

New suppliers route through a dedicated approval chain before any PO can be raised. Limit which suppliers each requester can use. Automation removes the option to skip the step or change the predefined procedure.



Bill duplicate detection · prevents double payments

Cross-checks supplier, date, and amount across incoming bills. If two appear to duplicate, approvers are notified instantly — review, approve or reject, no double payment lands.



2FA, auto-logout, and bypass-detection alerts

Two-factor authentication on every account. Auto-logout after 15 minutes of inactivity. Real-time admin notifications for any document approved directly in the ledger or changed after approval — by amount, contact, account, or category.

SECTION 10

Fraud prevention checklist.

Five improvement areas, designed to be ticked by hand and reviewed quarterly. Print this page, share it across the AP function, and use it as a baseline before your next internal audit.

01 Educate employees

- ◯ Hold mandatory training for all employees on how AP fraud affects the business and how they can prevent it.
- ◯ Include industry-specific examples that mirror the responsibilities of your actual staff.
- ◯ Set up recurring training and update content as new fraud methods emerge.

02 Segregate tasks and approvers

- ◯ Split invoice review and payment execution so each task is performed by two different people.
- ◯ Build a delegated financial authority (DFA) matrix that defines approvers and limits at every level.

03 Watch out for the red flags

- ◯ Make the 17-flag list (page 07) part of security training and distribute it as a standing memo for the AP team.

04 Verify your vendors and suppliers

- ◯ Create a documented new-vendor verification process — entry and approval performed by two different people.
- ◯ Run a regular supplier audit; verify any dubious entries by phone, online, or in person.

05 Start using ApprovalMax

- ◯ Start a 14-day free trial of ApprovalMax to automate segregation of duties and reduce the risk of fraudulent activity. **app.approvalmax.com/register**

ApprovalMax

FROM CAPTURE TO APPROVAL TO PAYMENT

TAKE THE NEXT STEP

Verified, visible, and accounted for.

ApprovalMax is the governance layer that controls every dollar leaving your business — from capture to approval to payment. Built for finance leaders who want a defensible audit trail by default, not as an afterthought.

With ApprovalMax, your finance team moves faster, with more control.

- **Enforce delegation of authority** automatically — no policy memo, no manual checking, no exceptions.
- **Catch duplicates, bank-detail changes, and threshold splits** at the moment of approval, not on a Friday reconciliation.
- **Hand auditors a defensible trail** on day one — every approval, override, and exception captured and posted to the ledger.

APPROVAL VELOCITY, MEASURED

< 1 day

50% of bills routed through ApprovalMax are approved in under a day. 25% within two — without sacrificing a single control step.

Connect your accounting system, build your first approval workflow, and watch every payment leave with your permission.

Start free trial →

Book a demo

WORKS WITH XERO · QUICKBOOKS ONLINE · NETSUITE

approvalmax.com · 14-day free trial · No credit card required · Cancel anytime