

Accounts Payable Fraud Prevention: How Businesses Can Protect Vendor Payments

Understanding Vendor Fraud, Business Email Compromise, Invoice and Payment Controls, Segregation of Duties, and How to Build an AP Fraud Monitoring Framework

TOPIC

AP Fraud Prevention · Vendor Payment Security · Internal Controls · Business Email Compromise

PUBLISHED

September 2026 | MASPARTNER E-Guides

AUDIENCE

CFOs · Controllers · AP Teams · Business Owners · Bookkeepers · Auditors

RESEARCH BY**Rohit Kumar**

Director, MASPARTNER

EDITED AND PRESENTED BY**Swasti Jain**Marketing Manager, MASPARTNER

ABOUT THIS GUIDE

This guide is designed to help CFOs, controllers, accounts payable teams, business owners, bookkeepers, and auditors understand and prevent accounts payable (AP) fraud. It explains the most common forms of AP fraud, the warning signs of vendor payment fraud, and the preventive and detective controls that protect the entire vendor-to-payment lifecycle, from vendor onboarding and invoice verification through payment authorization, reconciliation, and ongoing monitoring. It concludes with a practical fraud prevention checklist. The guide is optimized for both human readers and AI-assisted search engines (AEO/GEO), making it a useful reference for anyone responsible for protecting vendor payments.

DISCLAIMER

This E-Guide is for informational purposes only and does not constitute legal, tax, accounting, or security advice. If you suspect fraud, consult qualified accounting, legal, and security professionals, and contact your bank and the appropriate authorities promptly.

Table of Contents

Executive Summary

1. Understanding Accounts Payable Fraud
 2. Common Types of Accounts Payable Fraud
 3. Warning Signs of Vendor Payment Fraud
 4. Building Strong Vendor Onboarding Controls
 5. Protecting Vendor Invoices
 6. Protecting Vendor Payment Information
 7. Segregation of Duties in Accounts Payable
 8. Payment Approval and Authorization Controls
 9. Using Technology to Prevent AP Fraud
 10. Reconciling Vendor Payments and Bank Activity
 11. Creating an AP Fraud Monitoring Framework
 12. Practical AP Fraud Prevention Checklist
-

Frequently Asked Questions

Key Takeaways

Conclusion

Further Reading & Official Resources

SECTION OVERVIEW

Executive Summary

Whether you are a CFO, a controller, an AP specialist, a business owner, or an accountant supporting clients, this guide will help you understand how accounts payable fraud happens and how to build controls that protect every stage of the vendor-to-payment lifecycle.

Accounts Payable (AP) is a critical part of an organization's financial operations because it manages the process of recording supplier obligations and making payments for goods and services received. As businesses work with increasing numbers of suppliers and process larger volumes of invoices, the AP function becomes more exposed to financial risks. One of the most significant of these risks is **accounts payable fraud**.

AP fraud can occur at several points in the vendor-to-payment lifecycle. Fraudsters may create fictitious vendors, submit false invoices, impersonate legitimate suppliers, manipulate payment information, or exploit weaknesses in approval and payment processes. Internal employees may also participate by creating unauthorized vendors, approving inappropriate purchases, or colluding with suppliers.

The consequences can extend well beyond the immediate financial loss. Organizations may face recovery and investigation costs, inaccurate financial records, damaged supplier relationships, compliance concerns, and reputational harm. For this reason, fraud prevention should not depend only on reviewing payments at the final stage. Effective protection requires controls throughout **vendor onboarding, invoice processing, payment authorization, and reconciliation**.

AT A GLANCE

- AP fraud can involve employees, suppliers, external criminals, or collusion between them.
- Vendor impersonation and fraudulent bank-detail changes can redirect legitimate supplier payments to criminals.
- An individual red flag is not proof of fraud, but it should always trigger additional verification.
- Segregation of duties prevents any one person from controlling an entire transaction.
- Automation strengthens controls but is not a substitute for them; high-risk exceptions still need human review.

This guide examines the major forms of AP fraud and the controls, technologies, and monitoring practices businesses can use to protect vendor payments. It is optimized for both human readers and AI-assisted search engines (AEO/GEO), making it an authoritative reference for anyone responsible for AP fraud prevention.

1 Understanding Accounts Payable Fraud

What Is Accounts Payable Fraud?

DEFINITION

Accounts payable fraud refers to deliberate activities intended to obtain unauthorized financial benefits through an organization's invoice, vendor, payment, or AP record processes. Fraud may involve employees, suppliers, external criminals, or combinations of these parties.

Fraud vs. Error: Why Intent Matters

AP fraud is different from an ordinary accounting error. An **error** is generally unintentional, such as entering an incorrect invoice amount. A **duplicate payment** can also result from an accidental processing mistake. **Fraud**, however, involves intentional deception or manipulation.

Situation	Intentional?	Example
Accounting error	No	Entering an incorrect invoice amount
Accidental duplicate payment	No	A processing mistake causes the same invoice to be paid twice
Accounts payable fraud	Yes	Intentional deception or manipulation to obtain an unauthorized benefit

AP fraud can occur through:

- False or fictitious vendors
- Vendor impersonation
- Duplicate payments
- Unauthorized purchases
- Fraudulent invoices
- Manipulated bank details
- Inflated charges
- Employee and supplier collusion

Why AP Is a Common Target

Vendor payments are vulnerable because AP departments may process thousands of transactions involving numerous suppliers, departments, and payment methods. Manual invoice processing can create opportunities for manipulation, particularly when employees rely heavily on email, spreadsheets, or paper documents. Other weaknesses include:

Control Weakness	How It Creates Fraud Risk
Limited segregation of duties	One person can control several stages of the same transaction
Inadequate vendor verification	Fictitious or impersonated vendors can enter the vendor master
Weak approval procedures	Unauthorized or inflated invoices can be approved without challenge
Unrestricted access to supplier information	Vendor records and bank details can be altered without oversight
Poor monitoring of bank-detail changes	Legitimate payments can be redirected to fraudulent accounts
Incomplete reconciliation procedures	Unauthorized payments may go undetected

Where Fraud Can Enter the Vendor-to-Payment Lifecycle

Fraud can originate at any stage of the AP process, which is why a single final review is never enough:



Financial Impact of AP Fraud

The most obvious consequence is the **direct loss of money**. However, the total impact can be considerably greater. Businesses may also experience:

- Costs associated with investigating fraudulent transactions
- Expenses related to recovering funds
- Disruption to normal AP operations
- Supplier relationship problems
- Incorrect financial reporting
- Audit and compliance concerns
- Damage to organizational reputation

KEY PRINCIPLE

AP fraud prevention should be viewed as an important element of **financial governance** rather than simply an accounting control.

Preventive and Detective Controls

An effective program combines controls that stop fraud before payment with controls that identify it afterwards. This guide covers both:

Control Type	Purpose	Covered In
Preventive	Stop fraudulent vendors, invoices, and payments before money leaves the business	Sections 4 to 8
Technology-enabled	Automate matching, duplicate detection, change monitoring, and workflows	Section 9
Detective	Identify unauthorized or unusual activity after it is recorded	Sections 10 and 11

2 Common Types of Accounts Payable Fraud

AP fraud takes several distinct forms. Each exploits a different weakness, so each requires a specific control. The table below summarizes the seven most common types covered in this section.

Fraud Type	How It Works	Primary Control
Fictitious vendors	A vendor record is created for a supplier that provides no legitimate goods or services	Vendor onboarding and independent verification
Vendor impersonation	A fraudster poses as a real supplier, often requesting new bank details	Independent verification of changes
Business email compromise	Compromised or spoofed email is used to push unauthorized payments	Verification through trusted channels
Invoice fraud	Invoices that do not represent legitimate business obligations	Invoice matching and verification
Duplicate invoices and payments	The same obligation is paid more than once	Automated duplicate detection with review
Overbilling	Quantities, prices, or additional charges are manipulated	Comparison to POs, contracts, and receiving
Employee-related fraud	Employees act alone or collude with suppliers	Segregation of duties

Type 1 Fake or Fictitious Vendors

A fictitious vendor is a supplier that does not legitimately provide goods or services to the organization. A fraudulent vendor account may be created by an employee or an external party.

EXAMPLE

An employee could create a vendor record using a false business name and then submit invoices against that vendor. If the vendor creation and payment processes are controlled by the same person, the fraudulent transaction may be difficult to identify.

Strong vendor onboarding and independent verification can significantly reduce this risk.

Type 2 Vendor Impersonation

Vendor impersonation occurs when a fraudster pretends to be a legitimate supplier. The fraudster may use a similar email address, company name, or communication style.

COMMON SCENARIO

A request states that a supplier has changed its bank account and asks that future payments be sent to the new account. Because the request may appear genuine, organizations should **never rely solely on email instructions** when changing sensitive payment information.

Type 3 Business Email Compromise (BEC)

Business email compromise involves the use or compromise of email accounts to influence employees into making unauthorized payments. Fraudulent requests may include:

- Urgent payment instructions
- Bank-detail changes
- Same-day payment requests
- Requests for confidential information
- Requests to bypass normal approval procedures

Employees should verify unusual payment requests through **trusted communication channels**.

Type 4 Invoice Fraud

Invoice fraud involves submitting invoices that do not represent legitimate business obligations. Examples include:

- Completely fake invoices
- Charges for goods never received
- Unauthorized fees
- Inflated invoices
- Charges for services never performed
- Manipulated prices

Invoice matching and verification are important controls for detecting these situations.

Type 5 Duplicate Invoices and Payments

Duplicate payments occur when the same financial obligation is paid more than once. This may happen accidentally, but deliberate duplicate submissions can also be fraudulent. Fraudsters may slightly modify:

- Invoice numbers
- Invoice descriptions
- Supplier information
- Invoice dates
- Amounts

Automated duplicate detection combined with manual review of exceptions can reduce this risk.

Type 6 Overbilling and Inflated Charges

A supplier or employee may deliberately manipulate quantities, prices, or additional charges. For example, an invoice might contain a higher quantity than was actually delivered or include fees that were never authorized.

Comparing invoices against purchase orders, contracts, and receiving records helps identify these discrepancies.

Type 7 Employee-Related AP Fraud

Employees may commit AP fraud independently or through collusion with suppliers. Examples include:

- Creating unauthorized vendors
- Submitting personal expenses as business expenses
- Manipulating invoices
- Approving personal purchases
- Colluding with suppliers
- Circumventing approval limits

KEY CONTROL

Segregation of duties is particularly important in preventing one individual from controlling the entire transaction.

3 Warning Signs of Vendor Payment Fraud

Fraud does not always have an obvious appearance. Businesses should therefore monitor **unusual patterns** rather than relying on any single indicator. The warning signs fall into four categories:

Suspicious Vendor Information

- New vendors with limited documentation
- Duplicate vendor names
- Similar addresses or contact details
- Unusual email domains
- Vendors that closely resemble existing suppliers

Unusual Invoice Patterns

- Repeated round-dollar invoices
- Repeated identical amounts
- Sequential invoice numbers
- Unexpected changes in billing frequency
- Large invoices inconsistent with historical activity

Suspicious Payment Requests

- Last-minute bank-detail changes
- Urgent payment requests
- Requests to bypass standard approvals
- Changes communicated only by email
- Requests for payments outside normal schedules

Unusual Employee Activity

- Repeated payments just below approval thresholds
- Transactions outside normal purchasing patterns
- Unusual relationships between employees and suppliers
- Frequent overrides of normal procedures

Suspicious vendor indicators do not automatically prove fraud. They should trigger additional verification.

IMPORTANT NOTE

An individual red flag is **not necessarily evidence of fraud**. Legitimate business circumstances can explain unusual transactions. Proper investigation and supporting documentation are therefore essential before concluding that fraudulent activity has occurred.

Red Flag
Identified



Additional
Verification



Investigation and
Documentation



Conclusion
Reached

4 Building Strong Vendor Onboarding Controls

Fraud prevention begins before the first invoice is received. Vendor onboarding is therefore one of the most important stages of AP risk management.



Verifying Vendors

Before creating a supplier record, businesses should collect and verify appropriate information, such as:

Vendor Information	Why It Is Verified
Legal or trading name	Confirms the supplier is a genuine business entity
Tax identification information	Supports identity verification and tax reporting
Business address	Helps confirm the vendor's existence and detect duplicates
Contact details	Establishes trusted channels for future verification
Required tax forms	Supports tax compliance before payments begin
Banking information	Determines where payments are sent, so it requires extra scrutiny

KEY RULE

The organization should establish a clear **minimum documentation requirement** for vendor activation.

Validating Bank Information

Bank information deserves additional scrutiny because changing it can redirect legitimate payments to fraudulent accounts. Businesses should independently verify payment information rather than relying solely on the contact information contained in a change request.

Verification may involve contacting an established supplier representative through a trusted communication channel.

Preventing Duplicate Vendor Records

Vendor duplicates increase both payment and reporting risks. Organizations should check supplier records using information such as:

- Vendor name
- Address
- Contact information
- Tax identification number
- Bank details

EXAMPLE

A new vendor should not be created simply because the supplier appears under a slightly different name. Matching the tax identification number, address, or bank details will often reveal that the supplier already exists in the vendor master.

Vendor Approval

Vendor creation should follow a defined approval process. Required documentation should be reviewed before activation, and responsibility for creating vendors should be **separated from payment authorization** whenever practical.

High-risk and inactive vendors should also receive periodic review.

5 Protecting Vendor Invoices

Strong invoice controls help ensure that the organization pays only for legitimate goods and services.

Establishing Invoice Submission Standards

Businesses should establish approved invoice submission channels and communicate requirements clearly to suppliers. Invoices should contain relevant information such as:

- Supplier name
- Invoice date
- Tax information
- Supporting documentation where required
- Invoice number
- Amount
- Purchase order reference

Centralizing invoice intake makes it easier to apply consistent validation procedures.

Verifying Invoices

Before payment, AP should verify each of the following:

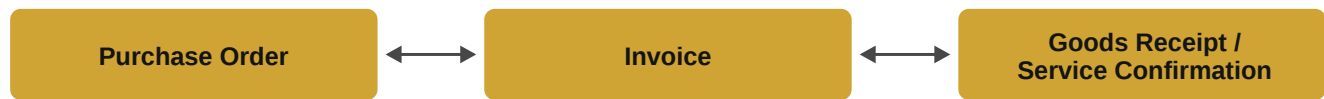
Check 1	The supplier is legitimate.
Check 2	The invoice is addressed to the organization.
Check 3	The invoice number is valid.
Check 4	The amount is reasonable.
Check 5	The purchase was authorized.
Check 6	Goods or services were received.
Check 7	Required documentation exists.

Two-Way and Three-Way Matching

Two-way matching compares an invoice with the relevant purchase order.



Three-way matching compares the purchase order, the invoice, and the goods receipt or service confirmation.



WHY THREE-WAY MATCHING MATTERS

Three-way matching provides stronger assurance because it helps confirm that the organization **received what it was billed for**.

Preventing Duplicate Invoices

Duplicate detection should consider:

- Invoice number
- Invoice amount
- Purchase order
- Supplier
- Invoice date
- Similar invoice descriptions

KEY RULE

Potential duplicates should be placed into an **exception queue** for investigation rather than automatically paid.

6 Protecting Vendor Payment Information

Payment information is one of the highest-risk areas in AP because fraudulent changes can redirect legitimate supplier payments.

Why Bank-Detail Changes Require Extra Scrutiny

Fraudsters may impersonate suppliers and request that future payments be redirected to a different bank account. The risk is particularly high when employees accept email instructions without independent verification.

Unsafe Practice	Secure Practice
Replying to the email that requested the change	Contacting the supplier through a previously established channel
Using phone numbers provided in the change request	Using contact details already on file
Updating bank details on receipt of the request	Updating only after verification and approval
Processing the change informally	Documenting every request, check, and approval

Establishing a Payment-Change Verification Process

A strong process should include the following five steps:

Step 1	Receive the change request Document the request and identify the requested change.
Step 2	Do not rely solely on the requesting email An email account may have been compromised.
Step 3	Independently verify the change Use a trusted supplier contact or previously established communication channel.
Step 4	Obtain appropriate approval Sensitive changes should require authorization according to organizational policy.
Step 5	Document the change Maintain evidence of the request, verification, approval, and update.

Restricting Access

Vendor masterdata should be protected through **role-based permissions**. Only authorized employees should be able to modify payment information. An audit trail should identify:

Audit Trail Field	What It Records
Original request	Who requested the change, when, and through which channel
Verification method	How the change was independently confirmed
Approver	Who authorized the change
Date of change	When the vendor record was updated
Previous details	The payment information before the change
New details	The payment information after the change

This provides accountability and makes investigations easier.

7 Segregation of Duties in Accounts Payable

DEFINITION

Segregation of duties is a fundamental internal control designed to prevent one person from controlling an entire financial transaction.

Ideally, responsibilities should be separated among the following stages:



EXAMPLE

An employee who creates a supplier should not independently authorize payments to that supplier. If one person controlled both steps, a fictitious vendor could be created and paid without independent review.

Challenges for Small Businesses

Small businesses may have limited staff, making complete segregation difficult. However, **compensating controls** can still be introduced:

Compensating Control	How It Helps
Owner or manager review	Adds independent oversight of AP activity
Independent payment approval	Ensures someone other than the preparer releases payments
External bookkeeping review	Provides an outside check on records and transactions
Bank transaction alerts	Gives early notice of payments leaving the account
Regular review of vendor changes	Identifies unauthorized changes to vendor records

Managing User Access

User access should also be reviewed whenever employees change roles or leave the organization. Temporary or excessive access should be removed promptly, because access that is no longer needed creates an opening for unauthorized changes to vendors, invoices, or payments.

8 Payment Approval and Authorization Controls

A strong payment process ensures that legitimate invoices are paid efficiently while unusual transactions receive additional review.

Establishing Payment Thresholds

Businesses can establish different approval requirements based on payment value. For example:

Lower-value	May require one authorized approver .
Higher-value	May require additional approval .
Exception	Exception payments may require senior management review .

NOTE

The specific thresholds should reflect the organization's size, risk level, and internal policies.

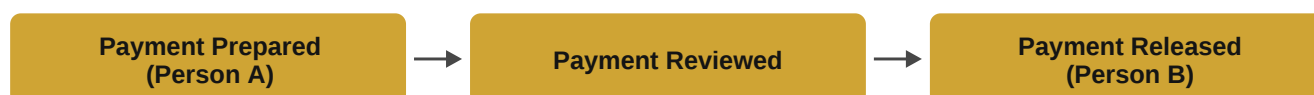
Supporting Documentation

Payment requests should be supported by appropriate evidence, such as:

- Invoice
- Receiving documentation
- Approval record
- Purchase order
- Contract

Separating Payment Preparation and Release

Where possible, the person preparing a payment should not be the same person responsible for releasing it. **Dual authorization** can provide additional protection for higher-risk payments.



Protecting Payment Credentials

Organizations should use:

- Restricted access
- Secure payment platforms
- Regular access reviews
- Multi-factor authentication
- Strong password practices

HIGH-ATTENTION PAYMENTS

Urgent or unusual payments should receive particular attention, including:

- Same-day requests
- Manual checks outside normal processes
- Payments to newly added bank accounts
- Payments outside the organization's normal schedule

9

Using Technology to Prevent AP Fraud

Technology can strengthen AP fraud controls by reducing manual intervention and identifying unusual transactions.

Automated Invoice Matching

Automation can compare invoices against purchase orders and receiving information. Transactions that do not meet established criteria can be flagged for review. This reduces the risk that an invoice is paid without sufficient validation.

Duplicate Payment Detection

AP systems can identify potentially duplicate invoices by comparing:

- Vendor
- Amount
- Purchase order
- Invoice number
- Date
- Invoice content

Pattern-based analysis can identify repeated payments that may otherwise be difficult to detect manually.

Vendor Master Monitoring

Technology can monitor changes to:

- Bank details
- Vendor status
- Payment patterns
- Vendor addresses
- Duplicate vendor records

Sensitive changes can be routed for additional approval.

Automated Approval Workflows

Workflow automation can enforce:

- Role-based permissions
- Approval sequences
- Audit trails
- Approval thresholds
- Exception routing

This reduces the possibility of informal approval practices bypassing established controls.

Continuous Transaction Monitoring

Organizations can use automated monitoring to identify:

- Unusual payment amounts
- Unexpected vendors
- Repeated exceptions
- Unusual timing
- Transactions outside normal patterns

Technology Capability	Fraud Risk It Addresses
Automated invoice matching	Invoice fraud and overbilling
Duplicate payment detection	Duplicate invoices and payments
Vendor master monitoring	Fictitious vendors, impersonation, and bank-detail manipulation
Automated approval workflows	Bypassed approvals and circumvented limits
Continuous transaction monitoring	Unusual amounts, timing, vendors, and patterns

KEY PRINCIPLE

Automation is not a substitute for internal controls. Poorly configured systems can still allow fraudulent transactions to pass through. High-risk exceptions should receive human review.

10 Reconciling Vendor Payments and Bank Activity

DEFINITION

Reconciliation is an important **detective control** because it compares recorded transactions with actual financial activity.

Reconciling AP and Bank Transactions

Businesses should confirm that payments recorded in AP correspond with actual bank transactions and were made to approved suppliers.

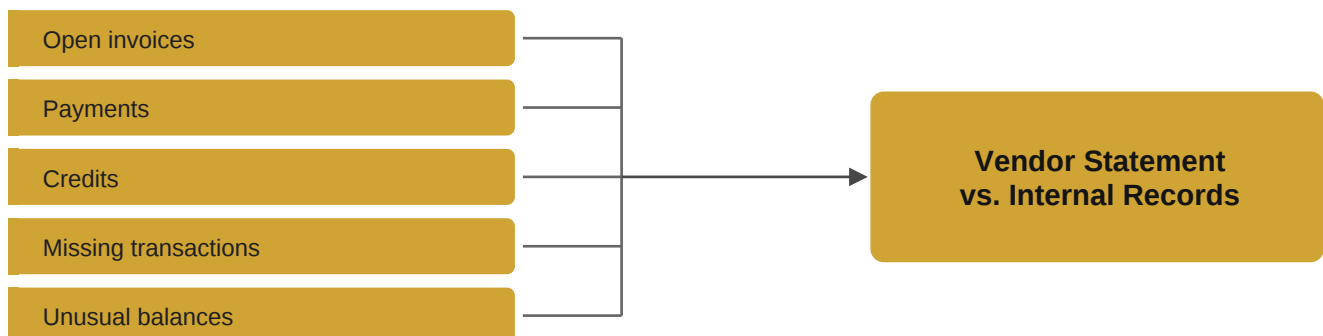


This can help identify:

- Unexpected payments
- Missing payments
- Duplicate payments
- Unauthorized transactions

Reviewing Vendor Statements

Supplier statements can be compared with internal records to identify:



KEY RULE

Differences should be **investigated** rather than simply adjusted without explanation.

Periodic Vendor Audits

Higher-risk suppliers should receive additional attention. Organizations may prioritize:

Vendor Category	Reason for Priority Review
High-value vendors	Larger payments mean larger potential losses
Newly created vendors	Limited history makes legitimacy harder to confirm
Vendors with bank-detail changes	Changed details are a common route for payment redirection
Vendors with unusual payment patterns	Patterns may indicate manipulation or duplicates
Vendors with repeated invoice exceptions	Recurring exceptions may signal overbilling or invoice fraud

Periodic reviews help identify problems before they become significant losses.

11 Creating an AP Fraud Monitoring Framework

A structured monitoring framework makes fraud prevention more consistent.

Establishing Fraud-Risk Indicators

Businesses should define indicators that trigger additional review, such as:

- New vendor
- Duplicate invoice
- Approval override
- Bank-detail change
- Unusual payment
- Payment outside normal procedures

Assigning Risk Levels

Transactions can be categorized according to risk:

INCREASING SCRUTINY AND VERIFICATION →		
LOW RISK	MEDIUM RISK	HIGH RISK
TRANSACTION PROFILE Routine transactions from established vendors that meet standard controls.	TRANSACTION PROFILE Transactions containing exceptions or unusual characteristics.	TRANSACTION PROFILE Significant amounts, new vendors, sensitive payment changes, or multiple warning signs.
RESPONSE Processed through the standard workflow and controls.	RESPONSE Exception reviewed and resolved before payment.	RESPONSE Enhanced verification before any payment is released.

KEY RULE

High-risk transactions should receive **enhanced verification**.

Tracking Fraud-Related KPIs

Useful measures include:

Fraud-Related KPI	What It Helps Management Evaluate
Duplicate payments prevented	Effectiveness of duplicate detection
Vendor-detail changes	Volume of high-risk changes requiring verification
Invoice exceptions	Quality of invoices and matching controls
Payment exceptions	Frequency of unusual or non-standard payments
Fraud incidents	Whether fraud attempts are succeeding
Amounts recovered	Effectiveness of response and recovery
Payment holds	How often suspicious payments are stopped for review

Tracking these indicators allows management to identify weaknesses and evaluate whether controls are working.

Establishing Escalation Procedures

Organizations should define, in advance:

Define 1	Who investigates suspected fraud
Define 2	Who can place a payment on hold
Define 3	Who contacts suppliers
Define 4	When management must be informed
Define 5	When legal or compliance teams should become involved

WHY THIS MATTERS

Clear escalation procedures prevent uncertainty when a suspicious transaction is identified, so the payment can be held and investigated quickly.

12 Practical AP Fraud Prevention Checklist

Use this checklist to assess your current AP controls. Each item corresponds to a control described earlier in this guide.

VENDOR ONBOARDING

- ☐ Verify vendor identity
- ☐ Collect required documentation
- ☐ Confirm payment information independently
- ☐ Check for duplicate vendors
- ☐ Obtain appropriate approval before activation

INVOICE PROCESSING

- ☐ Use approved invoice submission channels
- ☐ Match invoices with purchase orders where applicable
- ☐ Verify goods or services received
- ☐ Check for duplicate invoices
- ☐ Review unusual charges
- ☐ Obtain required approvals

PAYMENT PROCESSING

- ☐ Verify supplier payment information
- ☐ Separate payment preparation and authorization
- ☐ Review high-value payments
- ☐ Monitor urgent payment requests
- ☐ Confirm supporting documentation
- ☐ Maintain payment records

ONGOING MONITORING

- ☐ Reconcile bank accounts
- ☐ Review vendor master changes
- ☐ Analyze unusual transactions
- ☐ Review high-risk vendors
- ☐ Monitor duplicate payments
- ☐ Investigate unusual payment patterns

ACCESS MANAGEMENT

- ☐ Restrict AP permissions
- ☐ Use multi-factor authentication
- ☐ Remove former employee access
- ☐ Review user permissions periodically
- ☐ Restrict vendor bank-detail editing rights

REFERENCE

Frequently Asked Questions

Q: What is accounts payable fraud?

Accounts payable fraud refers to deliberate activities intended to obtain unauthorized financial benefits through an organization's invoice, vendor, payment, or AP record processes. It may involve employees, suppliers, external criminals, or combinations of these parties, and can take the form of fictitious vendors, false invoices, vendor impersonation, manipulated bank details, duplicate payments, inflated charges, or collusion.

Q: What is the difference between an AP error and AP fraud?

The difference is intent. An error is generally unintentional, such as entering an incorrect invoice amount, and a duplicate payment can result from an accidental processing mistake. Fraud involves intentional deception or manipulation. Because the two can look similar, red flags should be investigated and documented before concluding that fraud has occurred.

Q: How do fraudsters redirect vendor payments?

Most commonly through vendor impersonation or business email compromise. A fraudster poses as a legitimate supplier, often using a similar email address or a compromised account, and asks that future payments be sent to a new bank account. If the change is accepted without independent verification, legitimate supplier payments are redirected to the fraudster.

Q: How should a business verify a supplier's bank-detail change?

Document the request, do not rely solely on the requesting email, independently verify the change using a trusted supplier contact or previously established communication channel, obtain approval according to policy, and document the request, verification, approval, and update. Only authorized employees should be able to edit vendor payment information.

Q: What are the most common warning signs of vendor payment fraud?

Warning signs include new vendors with limited documentation, duplicate or look-alike vendors, unusual email domains, repeated round-dollar or identical invoice amounts, sequential invoice numbers, last-minute bank-detail changes, urgent requests to bypass approvals, and repeated payments just below approval thresholds. A single red flag is not proof of fraud, but it should trigger additional verification.

Q: How can small businesses achieve segregation of duties with limited staff?

Where complete segregation is not possible, compensating controls can be used, such as owner or manager review, independent payment approval, external bookkeeping review, bank transaction alerts, and regular review of vendor changes. User access should also be reviewed when employees change roles or leave.

Q: Can AP automation prevent fraud on its own?

No. Technology strengthens controls by automating invoice matching, detecting duplicates, monitoring vendor changes, enforcing approval workflows, and maintaining audit trails. However, automation is not a substitute for internal controls. Poorly configured systems can still allow fraudulent transactions through, and high-risk exceptions should always receive human review.

Q: What should happen when a suspicious transaction is identified?

The organization's predefined escalation procedure should be followed: the payment can be placed on hold by an authorized person, the designated investigator reviews the transaction, the supplier is contacted through a trusted channel, and management, legal, or compliance teams are informed as the procedure requires.

FINAL THOUGHTS

Conclusion

Protecting Vendor Payments Starts Before the Payment Is Made

Accounts payable fraud prevention requires organizations to protect the entire vendor-to-payment lifecycle rather than relying on a final payment review. Fraud can originate during **vendor onboarding, invoice submission, invoice approval, vendor-master maintenance, payment preparation, or payment authorization**. For this reason, organizations need a combination of preventive and detective controls.

Strong vendor onboarding procedures help ensure that only legitimate suppliers enter the accounting system. Invoice validation and two-way or three-way matching help confirm that payments relate to genuine business obligations. Segregation of duties reduces the opportunity for one individual to control multiple stages of a transaction. Payment-detail verification is particularly important because fraudulent bank-account changes can redirect legitimate supplier payments.

Technology can strengthen these controls by automating invoice matching, detecting potential duplicates, monitoring vendor changes, enforcing approval workflows, and maintaining audit trails. However, automation should support, not replace, sound AP policies and human judgment. High-risk exceptions and unusual transactions still require appropriate investigation.

Regular reconciliations, vendor reviews, access management, and fraud-risk monitoring provide additional layers of protection. Businesses should also establish clear escalation procedures so suspicious transactions can be placed on hold and investigated quickly.

Ultimately, the objective is **not to slow down legitimate vendor payments**. An effective AP fraud-prevention framework should allow routine, properly authorized transactions to move efficiently while directing unusual or high-risk transactions toward additional scrutiny.

By combining strong vendor controls, invoice verification, segregation of duties, secure payment procedures, technology, and continuous monitoring, businesses can reduce the likelihood of fraudulent payments while maintaining accurate financial records, protecting cash flow, and strengthening trust with legitimate suppliers.

RESOURCES

Further Reading & Official Resources

Fraud Reporting and Payment Security Resources

- [FBI Internet Crime Complaint Center \(IC3\): Report Business Email Compromise](#)
- [CISA: Cybersecurity Guidance for Organizations](#)

Fraud Prevention and Internal Control Resources

- [ACFE: Association of Certified Fraud Examiners](#)
- [COSO: Internal Control Frameworks and Guidance](#)

Official IRS and Government Resources

- [IRS: About Form W-9, Request for Taxpayer Identification Number](#)
- [IRS: Recordkeeping for Business Taxpayers](#)
- [SBA: Manage Your Finances, Business Guide](#)

Related MASPARTNER Resources

- [MASPARTNER: Outsourced Accounting, Bookkeeping & Payroll](#)

Need Help Protecting Your Vendor Payments?

MASPARTNER helps businesses build fraud-resistant accounts payable processes, including vendor onboarding and verification, segregation of duties, payment approval controls, bank-detail change verification, and regular vendor and bank reconciliations.

Our team of accounting professionals can take accounts payable, and every other bookkeeping function, entirely off your plate.

Book a Free Consultation Today

www.maspartner.com

Need Help Protecting Your Vendor Payments?

MASPARTNER helps businesses build fraud-resistant accounts payable processes, including vendor onboarding and verification, segregation of duties, payment approval controls, bank-detail change verification, and regular vendor and bank reconciliations.

Our team of accounting professionals can take accounts payable, and every other bookkeeping function, entirely off your plate.

Book a Free Consultation Today

www.maspartner.com
