SCAMSPOT BUSINESS

AP Fraud SOP Kit

Printable controls for suspicious invoices, vendor bank-account changes, business email compromise, callbacks, approval notes, and incident response.

The standing rule

Never change payment instructions or release a suspicious payment from email alone. Call the vendor on a number already in trusted records and require a second approver.

Use this kit when:

[ ] A vendor or supplier requests new bank, ACH, wire, routing, or IBAN details.

[ ] An invoice lacks a PO match or comes from a first-time vendor.

[ ] A sender uses urgency, secrecy, executive pressure, or an unusual payment rail.

[ ] The From, Reply-To, domain, or authentication result looks inconsistent.

[ ] A payment may already have gone to a fraudulent account.

Version 1.0 - July 2026
Free operational template. Adapt it with your finance, legal, security, and compliance teams.

1. Vendor bank-change verification policy

Apply this procedure to every change in payment instructions. Urgency, familiarity, letterhead, or a signed PDF never replaces independent verification.

[ ] Freeze the master-file change and hold payment.

[ ] Retrieve a trusted phone number from existing vendor records or a prior contract.

[ ] Do not use a phone number, link, or email address supplied in the change request.

[ ] Call a named finance contact and confirm the specific new account details.

[ ] Obtain confirmation from a second known vendor contact when possible.

[ ] Require a second internal approver before editing vendor master data.

[ ] Record who verified the change, the number used, its source, date, time, and result.

[ ] Apply a 24-48 hour hold before the next material payment when policy permits.

Verification record

Vendor / supplier	
Request received	
Trusted number source	
Contact 1 / outcome	
Contact 2 / outcome	
Internal approver	
Final decision	[ ] Approve [ ] Hold [ ] Reject [ ] Escalate

2. Fake invoice hold checklist

Hold the payment when any material item cannot be matched or verified.

Document and sender

[ ] Invoice number, amount, due date, tax details, and vendor identity match records.

[ ] From and Reply-To domains match expected vendor domains.

[ ] No unexpected portal, login page, QR code, attachment type, or shortened URL.

[ ] Payment instructions match prior paid invoices and vendor master data.

Purchase and receiving

[ ] A valid PO or approved internal requester exists.

[ ] Goods or services were received and match the invoice.

[ ] Quantity, price, tax, currency, and payment terms match the agreement.

Automatic hold triggers

[ ] New bank account, payment country, method, beneficiary, or remittance address.

[ ] Urgent same-day payment, secrecy, executive pressure, or threat of interruption.

[ ] Requester refuses a callback or insists on using contact details in the message.

[ ] First-time vendor without onboarding evidence or a named business owner.

[ ] Duplicate invoice number or a familiar invoice with changed payment details.

Decision

[ ] PAY - all required controls completed
[ ] HOLD - verification incomplete
[ ] REJECT - request contradicted by trusted records
[ ] ESCALATE - suspected compromise or funds already moved

3. Vendor callback script

Start the call from a number already in your records. Do not reply to the suspicious thread or call a number shown in the request.

Opening

Hi, this is [name] from [company] accounts payable. I am calling using the phone number already in our vendor records, not the number in the payment-change request.

Questions

1. We received invoice or payment request [reference] for [amount]. Is it legitimate?
2. Did your organization request a change to bank, ACH, wire, routing, IBAN, beneficiary, or payment method?
3. What are the exact authorized details and effective date?
4. Who authorized the change, and can a second known contact confirm it?
5. Has your team seen any mailbox compromise, forwarding rule, or impersonation warning?

Close

For security, we will keep the payment on hold until independent verification and our internal second approval are complete. We will not use contact details from the request.

Call record

Caller / role	
Number used / source	
Date / time	
Outcome / notes	

4. Internal approval note

Copy this structure into the payment approval trail or vendor master record.

Vendor	
Invoice / payment	
Amount / currency	
Risk posture	[ ] Low [ ] Review [ ] High
Observed flags	
Trusted verification	
Verifier / date	
Second approver	
Decision	[ ] Pay [ ] Hold [ ] Reject [ ] Escalate

Minimum evidence to retain

[ ] Original message with full headers and attachments preserved.

[ ] Prior invoice, PO, contract, and vendor master record used for comparison.

[ ] Callback record and source of the trusted contact details.

[ ] Names of the verifier and second approver.

[ ] Bank escalation or incident reference if funds moved.

5. First-hour incident response

If funds may have moved, time matters. Follow your organization's incident plan and contact qualified legal, financial, security, and insurance professionals.

[ ] Call the bank immediately and request a hold, recall, or fraud escalation.

[ ] Preserve the original email, full headers, attachments, invoice, and payment records.

[ ] Notify finance leadership, IT/security, legal, and cyber insurance contacts.

[ ] Contact the real vendor through a trusted channel.

[ ] Reset affected credentials, review mailbox forwarding rules, and revoke sessions.

[ ] Report US incidents to FBI IC3 and FTC ReportFraud; use local authorities elsewhere.

Primary references

FBI IC3 - 2025 Internet Crime Report

FTC - ReportFraud

APWG - Phishing Activity Trends

Google - Check whether a message is authenticated

ScamSpot limitation

ScamSpot provides risk indicators and operational templates. It does not verify vendors, bank-account ownership, invoice legitimacy, or authorization to move money.

Free online tools: scamspot.io/business/
Invoice check: scamspot.io/business/invoice-scam-check/
Email header checker: scamspot.io/email-header-checker/