JCPIT | SUPPORT
KEEPING IT SIMPLE

FINANCE AND PAYMENT CONTROL

Invoice fraud checklist.

A simple payment process for verifying changed bank details and acting quickly when something is wrong.

PREPARED BY
JCPIT Support Pty Ltd

USE THIS COPY
Owner: ________ Edition: July 2026

JCPIT | SUPPORT
KEEPING IT SIMPLE

PAUSE, VERIFY, APPROVE

Before money leaves

CHECKLIST · 01

Use this whenever supplier bank details change, a payment is unusual, or a request arrives with secrecy or urgency.

BUSINESS	PAYMENT PROCESS OWNER
PRIMARY APPROVER	BACKUP APPROVER
TRUSTED SUPPLIER RECORDS KEPT IN	NEXT PROCESS REVIEW

01

PRIORITISED FIRST STEP

Freeze the change and call a trusted number.

Use a number already held in your supplier file or a verified contract. Never use the number printed on the changed invoice or in the message that requested the change.

1 Verify changed bank details

- [ ] Call the supplier using a trusted record that existed before the request.
- [ ] Ask a known supplier contact to confirm the request and read the account details back.
- [ ] Record who confirmed the change, the trusted number used, the date and the time.
- [ ] Check that the requester is authorised to change payment details.
- [ ] Treat secrecy, urgency or instructions not to call as reasons to stop, not reasons to rush.

VERIFIER ____________ SUPPLIER RECORD / CALL NOTE ____________

2 Separate entry from approval

- [ ] A second authorised person checks every bank-detail change before it is used.
- [ ] Large or unusual payments receive a second review against the order, invoice and supplier record.
- [ ] The person approving uses their own account. No shared passwords or approval by informal text.
- [ ] A documented backup approver keeps the process working when someone is away.

FINANCE OWNER ____________ SECOND APPROVAL FROM $ ____________

ACCOUNTS, EVIDENCE, RESPONSE

Close the gaps

CHECKLIST · 02

3 Protect finance accounts

- [ ] Turn on multi-factor authentication for email, banking and accounting accounts.
- [ ] Use individual accounts and restrict who can edit suppliers or release payments.
- [ ] Enable change alerts and keep the accounting or payment system audit trail.
- [ ] Remove access promptly when staff leave or roles change.

SYSTEM OWNER ____________ SETTINGS / REVIEW DATE ____________

4 If the request looks suspicious

- [ ] Pause the payment and tell the finance owner through a trusted channel.
- [ ] Keep the original email, invoice, message headers, call details and payment records.
- [ ] Ask your IT provider to check the mailbox, sign-ins, forwarding rules and sent items.
- [ ] Warn the real supplier using a trusted contact if their identity or mailbox may be involved.

INCIDENT CONTACT ____________ EVIDENCE FOLDER ____________

5 If money has already been sent

- [ ] **Call the bank immediately** and ask for its fraud and transfer recall process. Record the case number.
- [ ] Contact your IT provider if email or an account may be involved. Preserve evidence before making broad changes.
- [ ] Follow your insurer's instructions and report the incident through ReportCyber. Follow the current reporting guidance. Call 000 if anyone is in immediate danger; otherwise contact police when the guidance directs you to.
- [ ] Record what happened, who acted and what control will change before the next payment.

RESPONSE LEAD ____________ BANK CASE / INCIDENT RECORD ____________

QUARTERLY PROCESS CHECK

SAMPLE CHANGE TESTED	ACCESS REVIEWED	NEXT TEST DATE
____________	____________	____________

A SECOND SET OF EYES

Check the payment controls.

JCPIT can review email access, sign-in protection and the controls used to approve supplier changes. You receive a short list of gaps and owners.

jcpit.com.au/free-security-check/
(03) 9021 0890

A convincing invoice is not proof. The control is the separate verification and approval process. Store the completed checklist securely. Do not record passwords, authentication codes, full bank details or unnecessary personal information.