Business Email Compromise

First-Response Checklist

Start finance and IT work together. Tick actions when complete and log decisions in the incident record.

Incident reference	Incident lead / initials	First report (date / time UTC)

On Receiving the Report

Finance | Stop payment fraud

- [ ] **Hold the payment**
  Hold related transfers and bank-detail changes. Check whether funds have left.
- [ ] **Contact the bank immediately**
  If funds moved, call the bank on its official number. Ask it to stop or recall the transfer. Save the case reference.
- [ ] **Verify the request separately**
  Call the supplier or colleague on a trusted number already held on file.

IT | Limit access

- [ ] **Preserve the original**
  Save the original email with full headers. Log receipt time and evidence reference.
- [ ] **Identify the affected account**
  Check for spoofing, supplier compromise or a breach of your mailbox. Verify with the owner on a trusted channel.
- [ ] **Contain credible account misuse**
  Ask an authorised admin to block sign-in and revoke sessions. Check app access separately. Log time and impact.

Scope, Evidence and Communications

- [ ] **Capture the state before changing it when safe**
  Save relevant sign-in, audit and mail-trace records. Record forwarding, rules, delegates and app access before removal. If harm is ongoing, contain immediately and log what changed.
- [ ] **Find and warn the people who may act on the message**
  Trace recipients and payment requests. Warn them via independently verified contacts. Record who was reached, how and when. Report fraud through the relevant UK police route.
- [ ] **Involve the privacy lead early**
  Record when you became aware of any personal data breach and assess risks to people. The controller must notify the ICO if required and document its decision. See the reporting test on page 2.

Before Restoring Access

- [ ] **Verify control, then reopen in stages**
  Verify the user through a trusted route. Reset credentials at their source, validate MFA methods and remove unauthorised access. Test sign-in and mail flow. Agree who will monitor for recurrence.
- [ ] **Release the payment hold separately**
  Finance independently verifies payment instructions and authorises release. Hand any open bank, recipient, privacy or monitoring actions to a named owner on page 2.

Shift Handover

Use references to restricted records. Keep message contents, personal details and bank details there.

Incident reference

Handover date and time (UTC)

Outgoing lead / initials

Incoming lead / initials

Current Position

Payment status / bank case reference

Accounts affected / containment times (UTC)

Original email, logs and before-change references

People warned / trusted route / time (UTC)

Evidence gaps and what remains unconfirmed

Privacy and Recovery Decisions

For a personal data breach, a controller must notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless risk to people is unlikely. If high risk is likely, inform affected people without undue delay. A processor must tell its controller without undue delay.

Awareness time / decision / risk record reference

Access and payment approvals / monitoring owner

Outstanding Actions

Record the next check, even when a third party owns the decision.

Next action or decision	Owner / initials	Due (date / time UTC)

Official guidance Payment fraud · UK fraud reporting · Microsoft 365 recovery · ICO breach guidance