CICADA | RESOURCES

LESSON 02 OF 03 · 7 MIN · WORKING KNOWLEDGE

Who to call, and when

Bank, insurer, IT, police, regulator. The order matters, and so do the deadlines.

The call list

- **Bank fraud line**: immediately if money has moved.
- **Insurer incident line**: often before you engage your own forensics; check the policy.
- **IT provider or incident responder**: to contain and investigate.
- **Legal adviser**: contracts, regulatory duties, communications.
- **Police / fraud reporting**: for a crime reference and investigation.
- **Regulator**: if personal data is involved and the threshold is met.

Store the numbers offline. A contact list inside the compromised mailbox is not a contact list.

Reporting duties

Rules vary by country and sector. In the UK, the ICO generally expects notification of a personal-data breach within 72 hours of becoming aware, where it's likely to result in a risk to people. US state laws vary; Australia's OAIC has its own scheme. Don't guess, check, and record your reasoning.

A police or fraud report gives you a reference that banks and insurers often ask for.

What to have ready

A short factual summary, the time detected, systems affected, data involved, actions taken, and who has been notified. Keep a decision log. Avoid speculation in writing and in public statements.

CALL THE INSURER EARLY

Many policies require notification before you appoint providers. Calling your own forensics first can jeopardise the claim. Read that clause before you need it.

Key takeaways

- ✓ Bank first if money moved; insurer early per policy.
- ✓ Keep contacts offline and verified.
- ✓ Know your breach -reporting deadline and threshold.
- ✓ Record decisions and notifications as you go.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.