First-hour incident response card

For a suspected cyberattack. Fill in trusted contacts and keep this card accessible offline.

If you suspect a fraudulent transfer, call the originating bank immediately.
Use a number from bank records. Hold related payments and ask about a recall.

Emergency contacts

Incident lead

Backup incident lead

IT responder

Operational safety lead

Bank fraud line

Alternate communication channel

Response checklist

- ☐ **Record and call.** Call your incident lead and IT using trusted numbers. Note what happened, who reported it and when.
- ☐ **Use a clean channel.** Switch to a known-clean device and an agreed phone or messaging channel outside the affected systems.
- ☐ **Contain safely.** Isolate affected devices from the network where safe. Involve the safety lead before disconnecting critical equipment. If ransomware is spreading and isolation is impossible, power down affected devices only if safe. This can lose evidence held in memory.
- ☐ **Preserve evidence.** Keep original messages, logs, timestamps and payment records. Limit access and record each action as it happens.
- ☐ **Secure affected accounts.** Have IT restrict access from a clean device, revoke sessions where supported, rotate exposed credentials and review recovery methods, forwarding and app access.
- ☐ **Assess and notify.** Record affected services, data and locations. Involve legal, privacy and insurance leads as appropriate. Assign notification owners and deadlines.
- ☐ **Start continuity.** Use an approved manual workaround. Have responders and service owners verify systems and workflows before reconnecting.

Incident notes

First report (time and zone)

Became aware (time and zone)

Affected workflow or payment and who is affected

Actions taken (time, person and action)

Next update (time and zone, audience and trusted channel)