CHECKLIST · SCAMS & SECURITY

Bell Direct and Bell Potter say some client data was likely accessed

Published 20 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/bell-financial-data-security-incident/

- [ ] **Note what Bell tells you.** If Bell contacts you about the incident, write down which of your details it says were involved.
- [ ] **Check any "Bell" message before acting.** Don't click links or call numbers in an unexpected text, email or call about your account. Use the contact details on belldirect.com.au or bellpotter.com.au.
- [ ] **Keep your password and one-time codes to yourself.** Don't give them to anyone who calls, texts or emails about the Bell incident.
- [ ] **Change reused passwords.** If you used your Bell password on any other site, change it there.
- [ ] **Check your account activity.** As a precaution, log in through the Bell website or app you normally use and look for trades or changes to your details that you didn't make.
- [ ] **Report suspected scams.** Report scam messages that use Bell's name to Scamwatch at scamwatch.gov.au.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.