CHECKLIST · SCAMS & SECURITY

Fortnum Private Wealth fined $1.35 million over cyber failures across its adviser network

Published 18 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/asic-fortnum-cybersecurity-penalty/

- [ ] **Ask your licensee for its cyber requirements.** If you run a practice as an authorised representative, get the current minimum controls in writing and confirm you meet each one.
- [ ] **Turn on multi-factor authentication.** Cover remote access and every system that holds client identity documents, tax file numbers or bank details.
- [ ] **Make cyber training mandatory.** Require cybersecurity training for every adviser and staff member, and record who has completed it.
- [ ] **Write and test an incident response plan.** Test it at least once a year, the standard ASIC pointed to in the FIIG Securities case.
- [ ] **Get specialist cyber expertise.** Employ or formally engage a person with specialised cybersecurity experience to help set and oversee your controls.
- [ ] **Plan your software updates.** Keep a schedule for patching the key systems your practice relies on, so security fixes aren't missed.
- [ ] **Monitor your network if you are a licensee.** Check how each authorised representative actually manages cyber risk, not just whether it has completed a self-assessment.

NOTES

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