Black Shard

RESEARCH REPORT

Australian notifiable data breaches, read for small and mid-sized firms

Attackers caused most of the breaches reported in 2025, and the sectors that hold health, financial and privileged client records reported the most. A small or mid-sized firm in those sectors defends the same information with fewer people.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-01
Classification	Public
Version	1.3
First published	14 July 2026
This edition	16 November 2026
Figures	OAIC figures of 6 Jul 2026, read 14 Jul 2026

Executive summary

The OAIC received 1,205 data breach notifications in the 2025 calendar year, up 8 per cent on 1,112 in 2024 and the most in any year of the scheme. That is 93 more notifications than in 2024, and more than three for every day of the year.

Malicious or criminal activity caused 716 of the 1,205 notifications, 59 per cent. The other 489 came from the scheme's two other causes, human error and system faults.

Health service providers made 225 notifications, 19 per cent of the total and the most of any sector. Financial services made 157, the Australian Government 118, business and professional associations 103, education 81, and legal, accounting and management services 81.

Each notification is an organisation that found a breach likely to cause serious harm to the people whose information it held, and reported it. For a small or mid-sized firm the sector table answers a practical question: whether the organisations that hold the same kind of information are being breached, and by what route.

Most breaches in the year came from attackers, so the controls that stop a stolen password or a malicious attachment carry most of the weight. The rest came from mistakes and faults, which a firm reduces with fewer people holding access, a list of where personal information sits, and a rehearsed first hour.

- Know where your personal, health and financial information sits, and who can reach it.
- Put phishing-resistant multi-factor authentication on email and every system that holds client records.
- Keep logs long enough to show what an attacker touched, and name the person who decides whether a breach is notifiable.

Method

Every figure comes from the release the Office of the Australian Information Commissioner published on 6 July 2026 with the Notifiable Data Breaches statistics for the 2025 calendar year. We opened and read the release on 13 and 14 July 2026 and print each figure as the OAIC states it.

Three figures are our arithmetic on the OAIC's own: the difference between the two years, the notifications not attributed to malicious or criminal activity, and the share made by the six largest sectors. Percentages are rounded to whole numbers, the way the OAIC rounds its own.

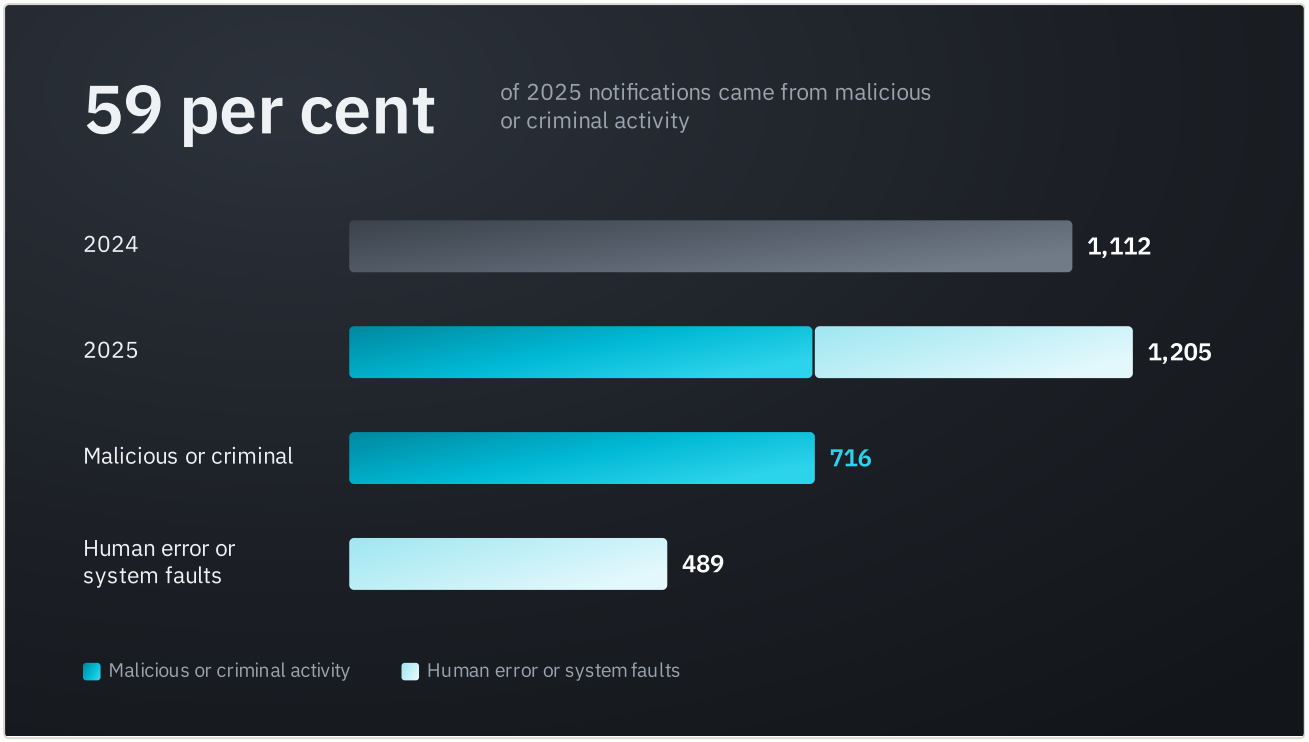
The scheme covers the agencies and organisations the Privacy Act binds. The Privacy Act's small business line sits at A$3 million in annual turnover, and a business that provides a health service and holds health information is covered whatever its turnover. A firm under the turnover line that suffers a breach is often outside the count, so the figures understate what happens to the smallest businesses.

Notifications are counted by the sector of the organisation that made them. Where several organisations hold the same breached information, one may notify for all of them, so a single notification can stand for a breach that reached many firms.

A record year

The OAIC received 1,205 data breach notifications in the 2025 calendar year, up 8 per cent on 1,112 in 2024 and the most in any year of the scheme. That is 93 more notifications than in 2024, and more than three for every day of the year.

NOTIFICATIONS AND THEIR CAUSES, 2024 AND 2025



Malicious or criminal activity caused 59 per cent of the 2025 notifications. Source: OAIC Notifiable Data Breaches statistics for 2025, published 6 July 2026.

Malicious or criminal activity caused 716 of the 1,205 notifications, 59 per cent. The OAIC names cyber attacks as the main route into those breaches.

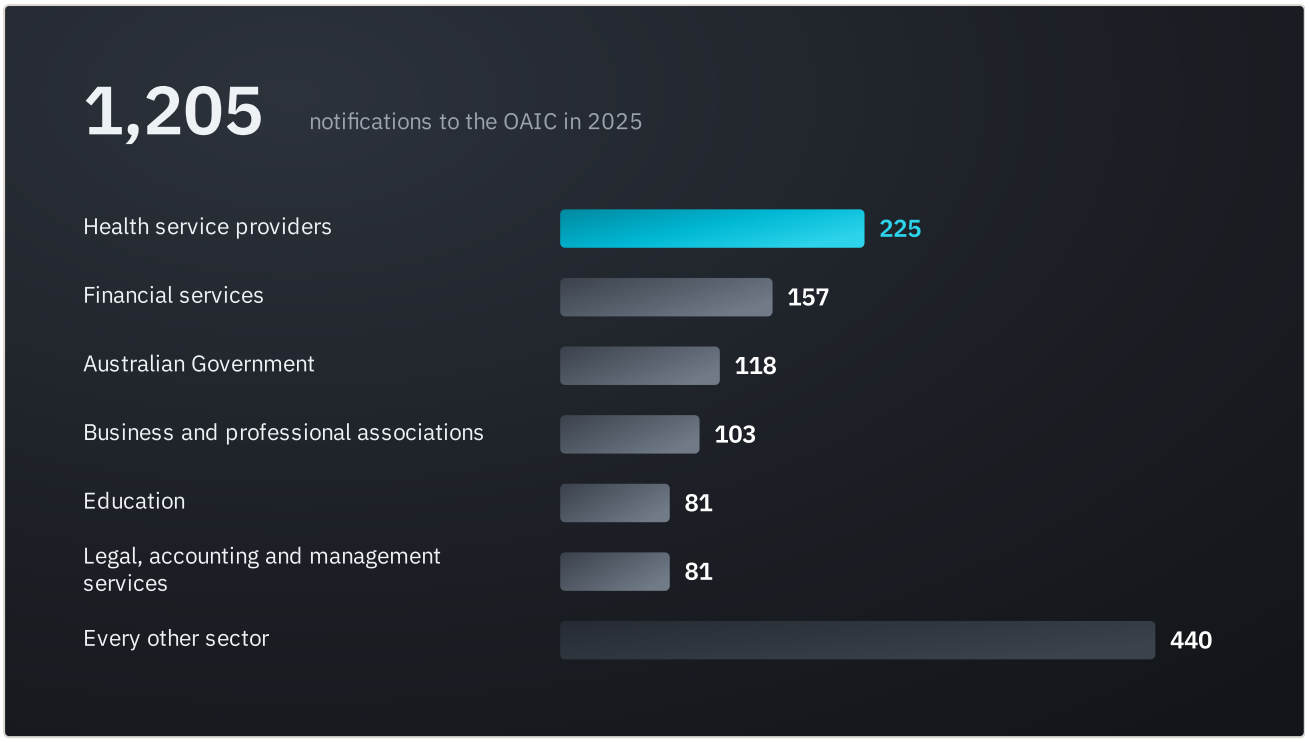
The other 489 came from the scheme's two other causes, human error and system faults. Human error covers the email sent to the wrong person, the spreadsheet attached by mistake and the file share left open. System faults cover software and processes that release information without anyone choosing to.

The split matters for a small firm because the two kinds of breach are stopped by different things. An attacker is stopped by identity controls, patching and the ability to see and contain what they do. Error and fault are reduced by holding less, sending less and checking what leaves the business.

The sector table

Health service providers made 225 notifications, 19 per cent of the total and the most of any sector. Financial services made 157, the Australian Government 118, business and professional associations 103, education 81, and legal, accounting and management services 81.

NOTIFICATIONS BY SECTOR, 2025



Health service providers notified the most breaches; the six largest sectors made 63 per cent of the year's notifications. Source: OAIC Notifiable Data Breaches statistics for 2025, published 6 July 2026.

The six largest sectors made 765 of the 1,205 notifications, 63 per cent; every other sector together made 440. The six share one trait: each holds information whose exposure is likely to cause serious harm, which is the test that makes a breach notifiable. Health records, account details, identity documents and privileged client files are the information attackers can sell or use, and the information a regulator expects to be guarded.

What the figures mean, sector by sector

Health service providers

Health led the table. Specialist rooms, clinics, allied health practices and the software they run hold diagnoses, referrals, Medicare details and next of kin, often in practice systems licensed from a vendor and in inboxes that receive results by email.

The Privacy Act reaches every business that provides a health service and holds health information, whatever its size, so the smallest practice carries the same notification duty as a hospital group. The routes in are usually a mailbox taken over through a phishing page, a remote access tool left open to the internet, or a supplier's platform breached upstream.

First moves: phishing-resistant sign-in on every mailbox, including shared ones; a list of every system and supplier that holds patient information; backups a compromised administrator cannot delete; and a written answer to who calls the OAIC.

Financial services

Advisers, brokers, fund managers and lenders hold identity documents, tax file numbers and account details, and move money on instructions that arrive by email. Business email compromise, where an attacker changes the bank

details on a payment request, is the breach that also costs money on the day.

Licensees are expected to manage cyber risk as part of their general obligations, and an APRA-regulated customer works under CPS 234, which holds it responsible for information assets its suppliers manage. A small firm that serves a regulated entity will be asked to show its controls before it is paid.

First moves: verify every change to payment details by calling a number already on file; separate administrator accounts; investor and client identity checks that fail closed when the check cannot run.

Australian Government

Agencies notify under the same scheme, and much of what they hold sits with contractors. Commonwealth entities are held to the Essential Eight under the Protective Security Policy Framework, and they pass that expectation to the suppliers who handle their information through contract clauses, security questionnaires and audit rights.

First moves for a supplier: an Essential Eight position measured against live systems, a named incident contact, and a clear statement of where government information is stored and who can reach it.

Business and professional associations

Associations hold member registers with contact details, payment records, qualifications and sometimes complaints, usually in a hosted membership platform run by a small team. A breach exposes people who joined for a credential, and it lands on a board of volunteers.

First moves: multi-factor authentication on the membership platform and its administrator accounts, a supplier clause that commits the platform to tell you about a breach quickly, and a short record of what the register holds and why.

Education

Schools, training organisations and tutoring businesses hold student records, parent contacts, health plans and fee accounts across learning platforms, enrolment systems and shared drives. Many breaches start in a third-party platform used by thousands of institutions at once.

First moves: an inventory of every platform that holds student information, single sign-on with multi-factor for staff, and retention rules so old records are deleted on schedule.

Legal, accounting and management services

Law firms, accountants and consultancies hold privileged files, tax affairs, trust account records and identity documents gathered for client checks. Since 1 July 2026 legal and accounting practices that provide designated services also carry AML/CTF obligations, which add identity records and suspicious matter reports to what they hold.

The common breach is a mailbox: an attacker reads the correspondence for weeks, then sends settlement or invoice details from a lookalike or a compromised account. Practice systems licensed from a vendor and document portals shared with clients are the next route.

First moves: phishing-resistant sign-in on every account, a rule that bank details are confirmed by phone, Conditional Access that blocks sign-ins from unmanaged devices, and an audit log of who opened which matter.

Every other sector

Retail, real estate, recruitment, insurance, telecommunications and the rest made the remainder. The pattern holds across them: the breaches that reach the OAIC are the ones where personal information was held in quantity, reached through a stolen credential or an exposed service, and noticed late.

What to do

An entity that suspects an eligible data breach has 30 days to assess it, then must notify the OAIC and the people affected as soon as practicable. The work that decides how those days go is done before the breach.

1. Write down which systems hold health, financial and identity information, who can reach each one, and which suppliers hold copies.
2. Enforce phishing-resistant multi-factor authentication on email, remote access and every system on that list, with the exceptions named and dated.
3. Keep sign-in and access logs long enough to answer the question the assessment asks: what did the attacker see.
4. Name the person who decides whether a breach is likely to cause serious harm, and the deputy who decides when they cannot be reached.
5. Draft the notice to the OAIC and the notice to affected people now, with the facts left blank.
6. Confirm every change to payment details by calling a number you already hold.
7. Make backups that a compromised administrator account cannot delete, and time a restore.
8. Ask each supplier that holds your clients' information how and when it will tell you about a breach, and put the answer in the contract.

Our free breach notification helper walks through the serious harm assessment in the browser, with nothing sent to us. A firm that wants the work done can engage our breach remediation team, which contains the incident, establishes what was reached and supports the assessment and the notices.

Our record

Black Shard builds and defends the systems Australian organisations run on.

The record is as held at 16 November 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Approved supplier on the Tasmanian Government Technology Services List (TSL) for Application Development Services, Operational Technical Services and Cyber Security.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.

- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 27 April 2026.

> 24/7 incident line: 1800 370 270.

Sources

- OAIC, Data breach notifications increase to all-time high in 2025, new NDB stats show, 6 July 2026: https://www.oaic.gov.au/news/media-centre/data-breach-notifications-increase-to-all-time-high-in-2025,-new-ndb-stats-show
- OAIC, Notifiable Data Breaches scheme: https://www.oaic.gov.au/privacy/notifiable-data-breaches
- Privacy Act 1988 (Cth), Part IIIC