

Data Breach Response Plan

How to contain, assess, notify and review a data breach involving personal information, aligned to the Privacy Act Notifiable Data Breaches scheme and OAIC guidance. Ready to adapt for your organisation.

Version 1.0 · October 2026 · Free template from Risk Frameworks Australia (riskfa.com) · No membership or sign-up

How to use this industry plan. Adopt the structure, terms and steps as written, so that your organisation responds to data breaches in the same language as the Privacy Act, the OAIC and the rest of the industry. Fill in the text in [square brackets] with your organisation's details, set the internal timeframes to match your size and risk appetite, delete obligations that do not apply to you, and approve the Plan through your governance process. Legal requirements are summarised as at October 2026: confirm the current requirements that apply to your organisation before relying on them, and get legal advice during a real breach. This template is general information only, provided free of charge, and is used at your own risk (see the disclaimer at the end).

Document control

Item	Detail
Document	Data Breach Response Plan
Organisation	[Organisation name]
Document owner	[Privacy Officer / Head of Compliance]
Approved by	[Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least [annually], after every eligible data breach or significant suspected breach, after each test, and after any material change in law or the business
Parent policy	[Privacy Policy (internal) / Information Security Policy / Incident & Issues Management Standard]

1. Purpose

This Plan sets out how [Organisation] responds to a **data breach** involving personal information. It ensures that:

- breaches are reported internally straight away and contained quickly to limit harm;
- every suspected eligible data breach is assessed reasonably and expeditiously, within the 30-day limit in the *Privacy Act 1988* (s26WH);
- the OAIC and affected individuals are notified as soon as practicable when an eligible data breach has happened (ss26WK, 26WL);
- affected customers get practical help to protect themselves from fraud, scams and identity misuse;
- other regulators (APRA, ASIC, ASD) and law enforcement are told within their own deadlines; and
- the causes are fixed and lessons are learned, so that breaches do not recur.

The Plan follows the four key steps in the OAIC's *Data breach preparation and response* guide: **contain, assess, notify, review**. It supports [Organisation]'s obligations under Australian Privacy Principle (APP) 11, Part IIIA (credit reporting), the *Privacy (Tax File Number) Rule 2015*, the Consumer Data Right where it applies, and APRA CPS 234 *Information Security* and CPS 230 *Operational Risk Management*.

2. Scope

This Plan applies to:

- all employees, contractors, directors and officers of [Organisation] and its subsidiaries;
- all personal information [Organisation] holds, in any form (electronic or paper), including customer, employee, applicant and third-party information;
- personal information held for [Organisation] by service providers, and personal information [Organisation] has disclosed to an overseas recipient where APP 8.1 applied (Privacy Act s26WC treats that information as still held by [Organisation]); and
- breaches caused by any means: cyber attack, insider misuse, human error (for example a misdirected email), lost or stolen devices or files, or a failure of a process or system.

A data breach that is also a cyber security incident is managed jointly with the RiskFA Cyber Incident Response Plan (section 6). Every data breach is also an incident under the RiskFA Incident & Issues Management Standard and is recorded in the incident register.

2.1 Which parts of the law apply to [Organisation]

Role	Information covered by the Notifiable Data Breaches scheme	Source
APP entity (most financial services organisations)	Personal information the entity must protect under APP 11.1	Privacy Act s26WE(1)(a)
Credit reporting body	Credit reporting information it must protect under s20Q	s26WE(1)(b)
Credit provider	Credit eligibility information it must protect under s21S(1)	s26WE(1)(c)
Tax file number recipient (for example employers, super funds, banks and investment bodies that collect TFNs)	Tax file number information it must protect under rule 11 of the <i>Privacy (Tax File Number) Rule 2015</i>	s26WE(1)(d); s26WB
Accredited data recipient or designated gateway under the Consumer Data Right	CDR data, which Part IIIC applies to as if it were personal information	<i>Competition and Consumer Act 2010</i> s56ES; OAIC CDR Privacy Safeguard Guidelines ch 12

Small business operators with an annual turnover of \$3 million or less are generally not APP entities (Privacy Act s6D), but some are still covered, for example credit reporting bodies (s6D(4)(f)) and AML/CTF reporting entities for their AML/CTF activities (s6E(1A)). The scheme also applies to credit providers and TFN recipients for that information. The *Privacy (Tax File Number) Rule 2015* is due to sunset on 1 April 2027 and is expected to be remade: check the current rule.

3. Key definitions

Term	Meaning
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded or not (Privacy Act s6).
Data breach	Any unauthorised access to, unauthorised disclosure of, or loss of personal information [Organisation] holds. Not every data breach is an eligible data breach.
Eligible data breach	Unauthorised access to, or unauthorised disclosure of, the information where a reasonable person would conclude that it would be likely to result in serious harm to any of the individuals to whom the information relates; or loss of the information in circumstances where unauthorised access or disclosure is likely to occur and, if it did, a reasonable person would conclude it would be likely to result in serious harm (s26WE(2)). Subject to the remedial action exception (s26WF).
Suspected eligible data breach	Where [Organisation] is aware that there are reasonable grounds to suspect that there may have been an eligible data breach, but is not aware of reasonable grounds to believe that there has been one (s26WH(1)). This triggers the assessment (section 11).
Reasonable person	In OAIC guidance, a person in the entity's position (not the position of an affected individual) who is properly informed, based on information immediately available or following reasonable inquiries.
Serious harm	Not defined in the Act. The OAIC describes it as including serious physical, psychological, emotional, financial or reputational harm. Assessed using the matters in s26WG (section 12).
At risk	An individual who would be likely to suffer serious harm from the eligible data breach (s26WE(2)(d)).
Remedial action	Action taken before serious harm occurs that means a reasonable person would conclude serious harm is no longer likely (or, for a loss, that no unauthorised access or disclosure happens). If it succeeds, the breach is not, and is taken never to have been, an eligible data breach (s26WF).
Statement	The statement about an eligible data breach that must be given to the OAIC and whose contents must be notified to individuals (ss26WK, 26WL).

Term	Meaning
Sensitive information	Includes health information and information about racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, and biometric information (s6).
Data Breach Response Team (DBRT)	The team in section 7 that leads [Organisation] 's response to a data breach.

Incident, Issue, Breach, Root cause, Extent of condition, Customer remediation, Critical operation, Material service provider and Reportable situation have the meanings in the RiskFA Incident & Issues Management Standard.

4. Legal and regulatory framework

Requirement	What it means for breach response
APP 11.1 and 11.2 (Privacy Act Sch 1)	Take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure; destroy or de-identify information no longer needed. APP 11.3 (added by the <i>Privacy and Other Legislation Amendment Act 2024</i> , in force 11 December 2024) confirms that reasonable steps include technical and organisational measures. A data breach often shows a possible APP 11 failure, which is assessed separately from notification.
Part IIIC, Notifiable Data Breaches scheme (ss26WA-26WU)	Assess suspected eligible data breaches within 30 days; notify the OAIC and individuals as soon as practicable; exceptions; Commissioner declarations and directions; OAIC information-gathering power (s26WU).
Part IIIA, credit reporting (ss20Q, 21S, 20K)	Security obligations for credit reporting bodies and credit providers; individuals who believe they are, or are likely to be, a victim of fraud can ask each credit reporting body for a 21-day ban period , which can be extended (s20K).
<i>Privacy (Tax File Number) Rule 2015</i> , rule 11	TFN recipients must take reasonable steps to protect TFN information and restrict access to it. A breach of the rule is an interference with privacy (Privacy Act ss 13(4), 18).
Consumer Data Right (<i>Competition and Consumer Act 2010</i> s56ES; Privacy Safeguard 12)	Accredited data recipients and designated gateways notify eligible data breaches of CDR data under Part IIIC.
Eligible data breach declarations (Privacy Act Part IIIC Div 5, ss26X-26XD)	After an eligible data breach, the Minister may declare that specified entities may collect, use and disclose specified personal information for specified purposes to prevent or reduce harm (section 18).
APRA CPS 234 <i>Information Security</i> (paras 23-26, 35, 36)	Detect and respond to information security incidents in a timely manner; maintain, annually review and test response plans; notify APRA within 72 hours of a material information security incident or one that has been notified to another regulator (para 35).

Requirement	What it means for breach response
APRA CPS 230 <i>Operational Risk Management</i> (paras 32, 41)	Notify APRA within 72 hours of an operational risk incident likely to have a material financial impact or a material impact on critical operations; within 24 hours of a disruption to a critical operation outside tolerance.
ASIC reportable situations (Corporations Act ss912D, 912DAA; NCCP Act ss50A, 50B; RG 78)	A data breach may involve a significant breach of a core obligation (for example the obligation to have adequate risk management systems). Assess and report within 30 days where it is a reportable situation.
<i>Cyber Security Act 2024</i> s27; SOCI Act ss30BC, 30BD	Ransomware or cyber extortion payment reports to the designated Commonwealth body (Home Affairs and ASD, lodged on cyber.gov.au) within 72 hours (annual turnover above \$3 million, or SOCI Part 2B responsible entities); cyber security incident reports for critical infrastructure assets within 12 or 72 hours.

5. Principles

1. **Report straight away.** Anyone who suspects a data breach reports it immediately. Staff are never penalised for reporting a genuine concern in good faith, including their own mistake.
2. **Contain first.** Act at once to stop the breach and limit harm. Containment does not wait for the assessment.
3. **Protect evidence.** Contain in a way that preserves logs, files and records needed for the assessment, regulators and law enforcement.
4. **The clock runs from awareness.** The 30-day assessment period runs from when [Organisation] is aware of reasonable grounds to suspect an eligible data breach, not from when an investigation starts or ends. The OAIC treats 30 days as a maximum, not a target.
5. **Assess honestly.** Consider the realistic harm to individuals, especially vulnerable customers. When in doubt, treat the breach as eligible and notify.
6. **Notify early and usefully.** Notification is a way to reduce harm. Tell individuals what happened and what practical steps they can take.
7. **Support customers.** Make it easy for affected customers to protect themselves, and never use a breach notice to sell products.
8. **One response, many obligations.** Coordinate privacy, prudential, conduct, cyber and law enforcement notifications so that messages are consistent and deadlines are met.
9. **Document everything.** Record facts, decisions, reasons and dates, including decisions not to notify.
10. **Learn.** Fix root causes and update controls, this Plan and training.

6. Relationship with other plans

Document	How it connects
RiskFA Cyber Incident Response Plan	Leads technical detection, containment, eradication and recovery for cyber security incidents. When a cyber incident involves, or may involve, personal information, the Cyber Incident Response Team activates this Plan at once and the two teams work together under one incident lead. This Plan leads the privacy assessment, notification and customer support.
RiskFA Incident & Issues Management Standard	Every data breach is recorded, rated (Critical, High, Medium, Low), escalated, investigated to root cause and closed under the Standard. Issues are raised for control gaps.
the RiskFA Crisis Management Plan and the RiskFA Business Continuity Policy	Activated for Critical breaches or where critical operations are disrupted.
the RiskFA Complaints Handling Policy and the RiskFA Customer Remediation Policy	Handle complaints and any compensation arising from a breach (ASIC RG 271, RG 277 where they apply).
[Third-party / Material Service Provider Policy]	Sets the breach notification, cooperation and audit terms in service provider contracts (CPS 230).

7. Data Breach Response Team and roles

The DBRT is convened by the [Privacy Officer] as soon as a possible data breach is reported, unless it is clearly minor and handled under section 9.2. Members can delegate to named alternates, recorded in Appendix A.

Role	Who	Responsibilities
DBRT lead	[Privacy Officer / Head of Compliance]	Runs the response; owns the assessment and the 30-day clock; recommends whether the breach is eligible and how to notify; keeps the decision log.

Role	Who	Responsibilities
Decision maker (eligible breach and notification)	[General Counsel] for High and Medium; [CEO] on [General Counsel] 's advice for Critical	Decides whether there are reasonable grounds to believe an eligible data breach has happened, and approves the OAIC statement and the notification option.
Legal	[General Counsel / external privacy lawyers]	Legal advice and privilege; secrecy and enforcement exceptions; declarations and applications to the OAIC; contracts and third parties; litigation risk.
Information security	[CISO]	Technical containment and forensic investigation with the Cyber Incident Response Team; evidence preservation; scope of compromised data; security measures and encryption assessment.
Technology and data	[Chief Technology Officer / Chief Data Officer]	Identify which systems and records are affected; extract and match the list of affected individuals; support recovery.
Risk	[Chief Risk Officer]	Rating under the Incident & Issues Management Standard; APRA materiality decision with Compliance; Board reporting.
Compliance and regulatory liaison	[Head of Compliance]	APRA, ASIC and other regulator notifications; consistent messages across regulators.
Customer and operations	[Head of Customer Operations]	Customer contact centre scripts, extra staff, identity verification and account security measures, vulnerable customer support, complaints.
Fraud	[Head of Fraud / Financial Crime]	Fraud monitoring on affected accounts; credential and payment controls; suspicious matter reporting where relevant.
Communications	[Head of Communications]	Customer notices, website statement, media and stakeholder messages, staff messages; approved by Legal.
People and Culture	[Chief People Officer]	Employee data breaches; staff support; insider matters.

Role	Who	Responsibilities
Third-party manager	[Relationship owner]	Coordinates with an affected service provider or partner entity (section 14).
Executive sponsor	[Accountable executive / CEO]	Approves resources and spending; informs the Board; accountable person where FAR applies.

The Board Risk Committee chair is told of any Critical data breach within [24 hours]. The Board receives a report on every eligible data breach.

8. Response overview and timeframes

The OAIC says the first three steps may happen at the same time or in quick succession. Internal targets are placeholders; set them to suit your organisation. Statutory limits are shown in bold.

Step	What happens	Internal target	Legal limit
Report	Anyone who suspects a data breach tells their manager and the [Privacy Officer] and records it (section 9).	Immediately; recorded within [same day]	The 30-day assessment clock may already be running from awareness
1. Contain	Stop the breach, recover the information, limit access, preserve evidence (section 10).	Started immediately; initial containment within [24 hours]	None stated; do it as quickly as possible
2. Assess	Initiate, investigate and evaluate whether there are reasonable grounds to believe it is an eligible data breach (sections 11 and 12).	Initial view within [72 hours]; decision within [10 business days] where possible	Reasonable and expeditious; all reasonable steps to finish within 30 days after becoming aware of reasonable grounds to suspect (s26WH)
3. Notify the OAIC	Prepare the statement and give it to the OAIC (section 13).	Within [2 business days] of the decision	As soon as practicable after becoming aware of reasonable grounds to believe (s26WK)

Step	What happens	Internal target	Legal limit
3. Notify individuals	Notify the contents of the statement to individuals using option 1, 2 or 3 (section 13).	Same time as, or within [2 business days] after, the OAIC	As soon as practicable after preparing the statement (s26WL(3))
Other notifications	APRA, ASIC, ASD, police, insurers, partners (section 15).	In parallel with the assessment	APRA 72 hours (CPS 234 para 35; CPS 230 para 32); ASIC 30 days ; others as in section 15
4. Review	Post-breach review, root cause, improvements (section 21).	Report within [20 business days] of closure of the response	None stated

9. Identify and report

9.1 How to report

- Any employee, contractor or service provider who suspects a data breach must report it **immediately** to their manager and to the **[Privacy Officer]** at **[privacy@organisation.com.au / phone]**, and through the **[incident register]**.
- Out of hours, report to the **[24/7 security operations centre / on-call duty manager]** on **[number]**, who contacts the **[Privacy Officer]**.
- Do not investigate further, delete anything, contact a suspected attacker, or tell customers until the DBRT says so, unless immediate containment is obvious and safe (for example recalling a misdirected email or asking the recipient to delete it).
- Record: what happened, when it happened and was found, how it was found, what information and how many people may be involved, what has been done so far, and who knows.

The OAIC says whether an entity is 'aware' is a question of fact, judged by how a properly informed reasonable person would act. Once a person responsible for compliance, or staff of appropriate seniority, know of information suggesting a breach, an assessment should start. Staff training must make clear that a delay in reporting can consume the 30-day assessment period.

9.2 Triage

Within **[4 hours]** of a report, the **[Privacy Officer]** triages it and records the outcome:

Outcome	Example	Action
Not a data breach	Information was sent to the right person; no personal information involved	Record and close.
Minor data breach, serious harm clearly not likely	A single low-sensitivity email to the wrong internal staff member, deleted unread	[Privacy Officer] contains, completes a short assessment in the register, and records why serious harm is not likely. No DBRT needed.
Possible eligible data breach, or uncertain	Any breach involving financial, identity, sensitive, TFN or credit information, more than [10] people, malicious actors, or media interest	Convene the DBRT within [2 hours] . Start the assessment clock record.
Cyber security incident with possible data exposure	Ransomware, compromised account, data exfiltration, extortion demand	Activate the RiskFA Cyber Incident Response Plan and the DBRT together.

10. Step 1: Contain

The OAIC's first step is to contain the breach: stop the unauthorised practice, recover the records, or shut down the system that was breached. Containment actions depend on the breach, and may include:

- isolating affected systems, disabling compromised accounts and credentials, blocking malicious traffic, and revoking access tokens and API keys (with the Cyber Incident Response Team);
- recalling misdirected emails; asking an unintended recipient to delete the information and confirm in writing that they have not used, copied or disclosed it;
- remotely locking or wiping lost devices; recovering lost files or documents;
- taking down information published online, and asking platforms or hosts to remove it;
- stopping a faulty process or system release that is exposing information;
- suspending a service provider's access, or asking the service provider to contain the breach under the contract; and

- putting extra fraud and identity checks on affected customer accounts at once (section 16).

Contain in a way that preserves evidence (section 20). Do not wipe or rebuild systems before forensic images and logs are secured, unless the CISO decides the immediate risk requires it and records the reason.

Paying a ransom or cyber extortion demand does not contain a data breach. Paying gives no assurance that stolen data will be deleted or not published, and the breach must still be assessed and notified. Any payment decision is made under the RiskFA Cyber Incident Response Plan, and a payment must be reported within 72 hours using the ransomware payment report form on cyber.gov.au (*Cyber Security Act 2024* s27, where the turnover threshold or SOCI Part 2B applies).

11. Step 2: Assess

11.1 The legal requirement

If **[Organisation]** is aware that there are reasonable grounds to suspect that there may have been an eligible data breach, it must carry out a **reasonable and expeditious assessment** of whether there are reasonable grounds to believe the circumstances amount to an eligible data breach, and take **all reasonable steps** to complete the assessment **within 30 days** after becoming aware (s26WH(2)). If **[Organisation]** already has reasonable grounds to believe there has been an eligible data breach, it moves straight to notification (s26WK) and does not wait for the 30 days.

11.2 How to assess

The OAIC suggests a three-stage process:

Stage	What the DBRT does
Initiate	Decide that an assessment is needed and who is responsible for it. Record the date [Organisation] became aware of the grounds for suspicion, and the 30-day deadline.
Investigate	Quickly gather the facts: what information was involved; how many and which individuals; how the breach happened and whether it is continuing; who has, or could have, the information; whether security measures such as encryption protected it; and what containment has achieved.

Stage	What the DBRT does
Evaluate	Decide, using the serious harm assessment (section 12 and Appendix B), whether there are reasonable grounds to believe there has been an eligible data breach, and whether remedial action has removed the likelihood of serious harm (s26WF). • Effort should be proportionate to the likelihood and apparent severity of the breach, but every step must move quickly. • Do not delay the decision to wait for perfect information: decide on the information available after reasonable inquiries. Where the facts show some individuals are at risk while the investigation continues for others, notify those already known. • If the assessment cannot be completed within 30 days, document the reasonable steps taken and the reasons for the delay, as the OAIC recommends. Consider telling the OAIC voluntarily. • Record the decision, the decision maker, the reasons and the date in the breach register (Appendix E), including a decision that the breach is not eligible.

11.3 Remedial action (s26WF)

If [Organisation] takes action before the breach results in serious harm and, as a result, a reasonable person would conclude that serious harm is not likely, the breach is not an eligible data breach and need not be notified. For a loss of information, the same applies if the action means there is no unauthorised access or disclosure. If remedial action works for some individuals only, those individuals need not be notified (s26WF(2), (5)). Examples from OAIC guidance: an unintended recipient confirms they deleted a file without opening it; a lost device is remotely wiped before anyone accessed it. Record the evidence that the remedial action worked. Assurances from a malicious actor (for example a promise to delete stolen data) are not reliable remedial action.

12. Serious harm assessment

In deciding whether a reasonable person would conclude that an access or disclosure would be likely, or would not be likely, to result in serious harm to any of the individuals, [Organisation] must have regard to the matters in s26WG. Use the worksheet in Appendix B.

s26WG matter	Questions to ask
--------------	------------------

s26WG matter	Questions to ask
(c) The kind or kinds of information	Identity documents (driver licence, passport, Medicare), account and card details, credentials, TFNs, credit information, health or other sensitive information, home addresses, combinations of information.
(d) The sensitivity of the information	Could it cause distress, discrimination, family violence risk or loss of safety? Is it about children or vulnerable customers?
(e) Whether security measures protect it	Was it encrypted, tokenised, hashed, password protected or access controlled?
(f) The likelihood that those security measures could be overcome	Is the encryption an industry-recognised secure standard? Were keys or passwords also compromised?
(g) Who has, or could obtain, the information	A trusted recipient who has confirmed deletion, an unknown party, a criminal group, a public website or dark web forum?
(h) If information was made unintelligible, the likelihood that people intending harm could get what they need to circumvent it	The Act notes that an encryption key is an example. The OAIC says that if an attacker holds both encrypted data and the key, the entity should not assume the data is secure.
(i) The nature of the harm	Identity theft, financial loss, fraud and scams, threats to physical safety, loss of employment or business opportunity, humiliation, damage to reputation or relationships, workplace or social bullying.
(j) Any other relevant matters	Scale and duration of exposure, whether the information is already being misused, the profile of affected individuals, how easily the information can be combined with other data.

OAIC guidance says that some kinds of information are more likely to cause serious harm if compromised, including sensitive information such as health information, documents commonly used for identity fraud, financial information, and combinations of personal information. In financial services, a breach of identity documents, account numbers with identifying details, or login credentials should be presumed to be likely to result in serious harm unless the DBRT records clear reasons why not.

13. Step 3: Notify

13.1 The statement to the OAIC (s26WK)

As soon as practicable after [Organisation] becomes aware that there are reasonable grounds to believe there has been an eligible data breach, it must prepare a statement and give a copy to the Commissioner. The statement **must** set out (s26WK(3)):

1. the identity and contact details of [Organisation] ;
2. a description of the eligible data breach;
3. the particular kind or kinds of information concerned; and
4. recommendations about the steps that individuals should take in response.

Where the breach is also an eligible data breach of other entities, the statement **may** also set out their identity and contact details (s26WK(4)). Lodge the statement using the OAIC's online Notifiable Data Breach form. The OAIC also expects, and its form asks for, further information such as the date or date range of the breach, the date it was detected, its cause, who has or may have obtained the information, and the containment and remediation steps taken. Use the template in Appendix C.

Preparing a statement that does not contain the four required items is a civil penalty provision for which the OAIC can issue an infringement notice or compliance notice (Privacy Act s13K(2), ss80UB, 80UC). Check every statement against Appendix C before it is lodged.

13.2 Notifying individuals (s26WL)

As soon as practicable after the statement is prepared, [Organisation] must notify its contents to individuals using one of three options (s26WL(2)):

Option	When it can be used	What to do
Option 1: notify all individuals	It is practicable to notify each individual to whom the relevant information relates	Take reasonable steps to notify the contents of the statement to every individual whose information was involved.
Option 2: notify only those at risk	It is practicable to notify each individual who is at risk from the breach	Take reasonable steps to notify the contents of the statement to each individual at risk of serious harm.

Option	When it can be used	What to do
Option 3: publish	Neither option 1 nor option 2 is practicable	Publish a copy of the statement on [Organisation] 's website and take reasonable steps to publicise its contents (for example social media, media releases, advertisements).

- [Organisation] may use the method it normally uses to communicate with the individual (s26WL(4)), for example email, SMS, app message or letter. Choose a method that will reach the person and that cannot easily be copied by scammers (section 16.2).
- The OAIC says it may be appropriate to tell individuals before or at the same time as the statement is given to the Commissioner, rather than waiting. [Organisation] 's default is to notify individuals at the same time as, or within [2 business days] after, the OAIC.
- Notify individuals in waves as they are identified; do not hold back notices until the whole affected population is known.
- The customer notice may include more than the statement, such as support offered and how to contact [Organisation] (Appendix D).
- [Organisation] may also choose to tell individuals about a breach that is not eligible, as good customer practice.

13.3 Exceptions and OAIC decisions

The following exceptions and OAIC powers are in Part IIIC. Legal must approve any reliance on an exception, and the reasons are recorded.

Provision	Effect
s26WD My Health Records	Part IIIC does not apply where the breach has been, or must be, notified under s75 of the <i>My Health Records Act 2012</i> .
s26WF Remedial action	Successful remedial action means the breach is not eligible, or certain individuals need not be notified (section 11.3).
s26WJ and s26WM Other entities	Where the same breach is an eligible data breach of more than one entity, an assessment or notification by one entity satisfies the others (section 14).

Provision	Effect
s26WN Enforcement related activities	Applies only to enforcement bodies: limits notification where it would be likely to prejudice enforcement related activities. Not usually relevant to financial services entities, but a law enforcement request to delay should be discussed with the OAIC (see s26WQ).
s26WP Secrecy provisions	Notification is not required to the extent it would be inconsistent with a secrecy provision of another Commonwealth law.
s26WQ Commissioner's declaration	On its own initiative or on application, the Commissioner may declare that notification is not required, or extend the time to notify individuals, having regard to the public interest and any advice from an enforcement body or ASD. While an application is being decided, ss26WK and 26WL do not apply (s26WQ(9)).
s26WR Commissioner's direction	The Commissioner may direct an entity to prepare a statement and notify individuals, after inviting a submission. The direction must be complied with as soon as practicable (s26WR(10)).
s26WS and s26WT	Exceptions to a direction for enforcement bodies and for secrecy provisions.
s26WU Information-gathering power	The Commissioner may require information, documents or answers about an actual or suspected eligible data breach and the entity's compliance.

Failing to assess (s26WH(2)), to give the statement to the OAIC (s26WK(2)), to notify individuals (s26WL(3)), or to comply with a direction (s26WR(10)) is an interference with the privacy of an individual (Privacy Act s13(4A)), which exposes [Organisation] to OAIC investigation, determinations and civil penalties (section 19).

14. Multiple entities, service providers and overseas recipients

- **Jointly held information.** Where information is held by more than one entity (for example [Organisation] and a service provider, a joint venture partner, a distributor or a product issuer), one entity's compliance satisfies the others: assessment (s26WJ) and notification (s26WM). But each entity remains responsible if no one complies.
- **Who notifies.** The OAIC suggests the entity with the most direct relationship with the individuals at risk should notify them. For [Organisation] 's customers this will usually be [Organisation] .
- **Contracts.** Agreements with service providers that hold personal information must require them to: tell [Organisation] of any suspected data breach within [24 hours] ; contain and preserve evidence; cooperate with the assessment; give [Organisation] the data needed to identify affected individuals; not notify individuals, regulators or the media about [Organisation] 's customers without agreement unless the law requires it; and meet the costs of their breaches as agreed. For APRA-regulated entities, this supports CPS 230 and CPS 234 requirements for service providers.
- **Overseas recipients.** Where [Organisation] disclosed personal information to an overseas recipient and APP 8.1 applied, a breach at the overseas recipient is treated as a breach of information [Organisation] holds (s26WC(1)). Similar rules apply to credit eligibility information disclosed to bodies with no Australian link (s26WC(2)).
- **Agree a joint plan.** Where several entities are affected, agree in writing who will assess, who will notify the OAIC and individuals, what each notice will say, and how customer enquiries are handled.

15. Other regulatory, law enforcement and external notifications

A data breach often triggers several notification obligations at once. [Head of Compliance] coordinates them so that each regulator gets consistent facts. Each decision to notify, or not, is recorded with reasons. The table summarises common obligations as at October 2026; delete those that do not apply.

Who	When it applies	Timing
APRA: information security incident (CPS 234 para 35)	APRA-regulated entities: an information security incident that materially affected, or had the potential to materially affect, the entity or customers, or that has been notified to another regulator (including the OAIC, in Australia or overseas)	As soon as possible and no later than 72 hours after becoming aware. As good practice, tell APRA no later than the OAIC notification.

Who	When it applies	Timing
APRA: operational risk incident (CPS 230 para 32) and critical operation disruption (para 41)	APRA-regulated entities: material financial impact or material impact on critical operations; critical operation disrupted outside tolerance. An incident notified under CPS 234 need not be notified again under para 32.	72 hours (para 32); 24 hours (para 41)
APRA: material information security control weakness (CPS 234 para 36)	The breach reveals a material weakness the entity expects it cannot remediate in a timely manner	10 business days after becoming aware
ASIC: reportable situation (Corporations Act ss912D, 912DAA; NCCP Act ss50A, 50B; RG 78)	AFS and credit licensees, where the breach is or may be a significant breach of a core obligation, or an investigation into one continues for more than 60 days (ASIC Instrument 2024/620, as described in RG 78)	30 calendar days after first knowing, or being reckless about, reasonable grounds to believe
ASD's Australian Cyber Security Centre	Cyber security incidents: voluntary reporting through ReportCyber (cyber.gov.au) is encouraged; mandatory for SOCI responsible entities (ss30BC, 30BD)	SOCI: 12 hours (significant impact) or 72 hours (relevant impact)
Ransomware or cyber extortion payment (<i>Cyber Security Act 2024</i> s27): the designated Commonwealth body (Home Affairs and ASD), using the report form on cyber.gov.au	Annual turnover for the previous financial year above \$3 million (s26(2); <i>Cyber Security (Ransomware Payment Reporting) Rules 2025</i> s6), or SOCI Part 2B responsible entities	72 hours after the payment or becoming aware of it
Police (state or territory police; AFP through ReportCyber)	Theft, extortion, fraud, insider misuse or other crime	As soon as practicable; consider any police request about the timing of notices

Who	When it applies	Timing
AUSTRAC (AML/CTF Acts 41)	Reporting entities that form a suspicion about a matter (for example fraud using breached data)	24 hours (terrorism financing) or 3 business days
Other privacy regulators	Breaches involving individuals in other jurisdictions (for example New Zealand, the EU or UK), or state or territory health records laws	As those laws require; get local advice
ASX (Listing Rule 3.1)	Listed entities, where information is price-sensitive	Immediately, unless an exception in LR 3.1A applies
Insurers	Cyber and professional indemnity policies	As the policy requires (often very short notice periods)
Card schemes, payment networks, credit reporting bodies, partner banks	Card or payment data, or where contracts require it	As the agreements require

This summary is general information and may not be complete for your organisation. The RiskFA Incident & Issues Management Standard has the full list of incident notifications. Confirm current requirements with the regulator's guidance or your legal adviser.

16. Supporting affected customers

16.1 Practical support

The recommendations in the statement must be practical and easy to act on. Depending on the information involved, **[Organisation]** should offer or recommend:

Information involved	Support and recommendations
Account numbers, card details or online banking credentials	Reset passwords and force re-authentication; reissue cards; extra monitoring and step-up verification on affected accounts; lower default limits or holds on unusual payments; tell customers how to set up multi-factor authentication.

Information involved	Support and recommendations
Identity documents (driver licence, passport, Medicare card)	Explain how to replace the document with the issuing agency, and offer to cover reasonable replacement costs [where approved] ; flag affected identities for extra checks on new applications and changes of details.
Name, date of birth, address with other identifiers	Explain that individuals can ask each credit reporting body for a free ban period (21 days, extendable) if they believe they are, or are likely to be, a victim of fraud (Privacy Act s20K); offer credit monitoring for [12 months] where the risk justifies it.
TFN	Tell individuals how to contact the ATO about protecting their tax records.
Health or other sensitive information	Provide information about relevant counselling and support services; take extra care with tone and channel.
Any breach with a risk of identity misuse	Refer individuals to an identity and cyber support service such as IDCARE (a not-for-profit identity and cyber support service for Australia and New Zealand). Referral is an option for [Organisation] to consider, not an endorsement, and any engagement should be agreed in advance.

- Set up a dedicated contact centre line, web page and FAQ before notices go out, with enough trained staff for the expected volume.
- Give vulnerable customers (for example those experiencing family violence, financial hardship, illness or language barriers) extra support. Where address or contact details are exposed for customers at risk of family violence, contact them directly and urgently about safety.
- Run targeted fraud monitoring on affected accounts and identities for at least [12 months], and track fraud linked to the breach.
- Handle complaints under the RiskFA Complaints Handling Policy, tell customers about AFCA, and consider compensation for loss under the RiskFA Customer Remediation Policy.

16.2 Protecting customers from scams that copy the breach

- Breach notices must **never** ask customers to click a link to log in, give a password or one-time code, or provide identity documents. Say so in every notice.
- Publish the notice on [Organisation]'s website so customers can check it is genuine, and tell customers how to contact [Organisation] using a known number.
- Warn customers that criminals may contact them pretending to be [Organisation], the police or a regulator.

17. Communications

- All external messages (customer notices, website statements, media, social media, partner and investor messages) are approved by [Head of Communications] and [General Counsel], and are consistent with the OAIC statement and regulator notifications.
- Use plain language: what happened, what information was involved, what [Organisation] is doing, what customers should do, and how to get help.
- Do not speculate, minimise or make assurances that cannot be supported (for example that stolen data has been destroyed).
- Brief staff, especially customer-facing staff, before customers are notified.
- Keep a single, dated record of every message and when it was issued.

18. Eligible data breach declarations

Since 11 December 2024 the Minister (the Attorney-General) may make an **eligible data breach declaration** after an eligible data breach of an entity, if satisfied it is necessary or appropriate to prevent or reduce a risk of harm from misuse of personal information following the breach (Privacy Act s26X). The declaration specifies the kinds of personal information, the entities that may collect, use or disclose it and receive it, and the permitted purposes (s26X(2)). Permitted purposes may include preventing or responding to cyber security incidents, fraud, scams and identity theft (s26X(5)). Media organisations cannot be specified as recipients (s26X(3)(b)). A declaration lasts no more than 12 months (s26XA).

- While a declaration is in force, an entity may collect, use or disclose personal information within its terms (for example to share details of compromised identities with other banks or government agencies) without breaching the APPs or the TFN rule (s26XB).
- A person who receives information because of a declaration commits an offence if they disclose it further, unless an exception applies (s26XC).

- **[Organisation]** must check for any declaration that covers a breach affecting its customers (whether its own breach or another entity's), and follow its conditions exactly. Legal approves any sharing under a declaration.

19. Why this matters: penalties and legal exposure

A data breach can expose **[Organisation]** to OAIC investigation and determinations, and to court proceedings for civil penalties. As at October 2026:

Provision	Summary
s13G Serious interference with privacy	Body corporate: up to the greatest of \$50 million , 3 times the benefit obtained, or (if the benefit cannot be determined) 30% of adjusted turnover in the breach turnover period (s13G(3)). The court may consider factors including the kinds and sensitivity of information, the number of individuals, whether a child or person experiencing vulnerability is affected, and whether the entity failed to implement practices, procedures and systems to comply with its privacy obligations (s13G(1B)).
s13H Interference with privacy (not serious)	Up to 2,000 penalty units, and up to five times that for a body corporate (<i>Regulatory Powers Act</i> s82(5)). Added by the 2024 amendments.
s13K Administrative tier	Includes a non-compliant s26WK statement (s13K(2)); up to 200 penalty units (five times that for a body corporate), and the OAIC can issue infringement notices (s80UB) and compliance notices (s80UC).
s80UA Court orders	Courts may make other orders after a civil penalty contravention, for example to redress loss or damage.
Statutory tort for serious invasions of privacy (Privacy Act Schedule 2, in force 10 June 2025)	Individuals can sue for a serious invasion of privacy, including misuse of information, where it was intentional or reckless. It is not a strict liability claim for every data breach, but it is relevant where, for example, an insider deliberately misuses customer information. Legal should assess exposure.

Other consequences include APRA supervisory action under CPS 234 and CPS 230, ASIC action where licence obligations are breached, contractual claims, class actions, and loss of customer trust. Accountable persons under FAR must take reasonable steps in their areas of responsibility.

20. Records and evidence

- The DBRT lead keeps a **decision log** from the first report: every fact learned, decision, decision maker, reason, and date and time.
- Record every data breach in the breach register (Appendix E), whether or not it is eligible, and link it to the incident register.
- Preserve evidence: forensic images, system and access logs, emails, the affected data set, and service provider reports. Keep a chain of custody record for evidence that may go to police or court.
- Where Legal directs that a forensic or investigation report be prepared for legal advice, follow Legal's instructions on privilege. Privilege does not remove the duty to give regulators the facts they are entitled to.
- Keep the list of affected individuals, notices sent, delivery results and contact centre records.
- Keep records for at least **[7 years]**, or longer where the law requires.

21. Step 4: Review

Once steps 1 to 3 are complete, the OAIC expects the entity to review and learn from the breach to improve its personal information handling. For every eligible data breach and every Critical or High data breach, the **[Privacy Officer]** leads a post-breach review, reported to the executive and the Board Risk Committee within **[20 business days]** of the end of the response. The review covers:

- the root cause and extent of condition, under the RiskFA Incident & Issues Management Standard (human error alone is never a root cause);
- whether APP 11 security steps (including technical and organisational measures) were reasonable, and what must change;
- whether **[Organisation]** held information it no longer needed (APP 11.2), and whether retention and destruction schedules were followed;
- service provider performance and contract gaps;
- how well this Plan worked: timeliness of reporting, containment, assessment and notification against section 8;
- the effectiveness of customer support and communications, using complaints and customer feedback; and
- issues and actions raised, each with an owner and due date, tracked to closure in the issues register.

Data breach themes are reported to the Board Risk Committee [quarterly], including near misses and breaches assessed as not eligible.

22. Preparedness, testing and training

- **Testing.** Test this Plan at least [annually] with a scenario exercise involving the DBRT, the Cyber Incident Response Team and the decision makers, and after major changes. APRA-regulated entities must annually review and test their information security response plans (CPS 234 para 26); include data breach scenarios.
- **Scenarios.** Vary them: ransomware with data theft and extortion; a service provider breach; a misdirected bulk email; an insider downloading customer data; a lost device; data found on a public website.
- **Readiness.** Keep contact lists, templates (Appendices C and D), the OAIC form link, legal and forensic retainers, and contact centre and mail-house arrangements ready and checked [half-yearly].
- **Data mapping.** Maintain an inventory of where personal information is held (including at service providers) so that affected individuals can be identified quickly.
- **Training.** All staff learn how to recognise and report a data breach at induction and [annually]. DBRT members receive role training [annually].
- **Assurance.** Second line reviews compliance with this Plan after each eligible data breach; Internal Audit reviews it at least every [3 years].

23. Related documents

- RiskFA Cyber Incident Response Plan; RiskFA Incident & Issues Management Standard
- [Privacy Policy], the RiskFA Cyber Security Policy, [Records Retention and Destruction Schedule]
- the RiskFA Crisis Management Plan, the RiskFA Business Continuity Policy, [Third-party / Material Service Provider Policy]
- the RiskFA Complaints Handling Policy, the RiskFA Customer Remediation Policy, [Fraud Management Policy]
- Privacy Act 1988: Part IIIC, Part IIIA, Schedule 1 (APPs), Schedule 2; *Privacy (Tax File Number) Rule 2015*
- OAIC: *Data breach preparation and response* guide; Notifiable Data Breach form; *Australian Privacy Principles guidelines* (chapter 11); *CDR Privacy Safeguard Guidelines* (chapter 12)
- APRA: CPS 234 and CPG 234; CPS 230 and CPG 230
- ASIC: RG 78 *Breach reporting by AFS licensees and credit licensees*; RG 271 *Internal dispute resolution*; RG 277 *Consumer remediation*
- Standards: ISO/IEC 27001 and 27002 *Information security*, ISO/IEC 27035 *Information security incident management*, ISO/IEC 27701 *Privacy information management*

Appendix A. First 24 hours checklist

#	Action	Owner	Done (time)
1	Breach reported to [Privacy Officer] and recorded in the incident register; reference number issued	Reporter / [Privacy Officer]	
2	Record the date and time [Organisation] became aware of grounds for suspicion; calculate the 30-day deadline	[Privacy Officer]	
3	Triage completed (section 9.2); DBRT convened if needed	[Privacy Officer]	
4	Cyber Incident Response Plan activated if a cyber incident is involved	[CISO]	
5	Immediate containment actions taken; evidence preserved	[CISO] / business owner	
6	Initial facts recorded: what, when, how, which systems, kinds of information, approximate number of individuals	DBRT	
7	Incident rated (Critical, High, Medium, Low) and escalated under the Incident & Issues Management Standard	[Chief Risk Officer]	
8	Legal engaged; privilege approach decided	[General Counsel]	
9	Service provider or other entity involvement identified and contacted	[Relationship owner]	
10	APRA 72-hour (and 24-hour) materiality decision made and recorded	[Head of Compliance]	
11	Insurers notified as the policy requires	[General Counsel / Risk]	
12	Police / ReportCyber considered	[CISO] / [Head of Fraud]	
13	Fraud monitoring and extra verification placed on potentially affected accounts	[Head of Fraud]	

#	Action	Owner	Done (time)
14	Holding statements prepared for staff, customers and media (not issued without approval)	[Head of Communications]	
15	Executive sponsor briefed; Board Risk Committee chair told if Critical	DBRT lead / [CRO]	
16	Decision log started and next DBRT meeting scheduled	DBRT lead	

Appendix B. Serious harm assessment worksheet

Question	Answer and evidence
Breach reference; date aware of grounds for suspicion; 30-day deadline	
Type of breach: unauthorised access, unauthorised disclosure, or loss	
Which entity role applies: APP entity, credit provider, credit reporting body, TFN recipient, CDR accredited data recipient (section 2.1)	
Kinds of information involved (s26WG(c)), listed by data field	
Sensitivity of the information (s26WG(d)); any children or vulnerable individuals	
Number of individuals and how many can be identified and contacted	
Security measures protecting the information (s26WG(e)) and the likelihood they could be overcome (s26WG(f), (h)), including whether keys or credentials were also exposed	
Who has or could obtain the information (s26WG(g)), and their likely intent	
Nature of the likely harm (s26WG(i)): financial, identity, physical safety, psychological, reputational, other	
Other relevant matters (s26WG(j)): evidence of misuse, publication, duration of exposure	
Remedial action taken and evidence it removed the likelihood of serious harm (s26WF), for all or some individuals	
Is the breach also an eligible data breach of another entity? Who will assess and notify (ss26WJ, 26WM)?	

Question	Answer and evidence
Conclusion: are there reasonable grounds to believe there has been an eligible data breach? Yes / No, with reasons	
Individuals at risk, and notification option (1, 2 or 3) with reasons	
Any exception relied on (section 13.3), with Legal's approval	
Decision maker, date and time	

Appendix C. Notification statement template (OAIC)

The first four items are mandatory under s26WK(3). The rest are what the OAIC expects and its form asks for. Lodge through the OAIC's Notifiable Data Breach form.

Field	Content	Required by
1. Identity and contact details of the entity	[Organisation legal name, ABN, address; contact name, role, phone and email for the breach]	s26WK(3)(a)
2. Description of the eligible data breach	[What happened, in plain words: how the information was accessed, disclosed or lost]	s26WK(3)(b)
3. Kind or kinds of information concerned	[For example: names, dates of birth, addresses, driver licence numbers, account numbers, TFNs, health information]	s26WK(3)(c)
4. Recommended steps individuals should take	[Practical, specific steps tailored to the information, for example: change passwords; replace identity documents; request a ban period from credit reporting bodies; watch for scams; contact us on a known number]	s26WK(3)(d)
5. Other entities involved (optional)	[Identity and contact details of other entities for which this is also an eligible data breach]	s26WK(4) (may include)
Date or date range of the breach; date detected	[dates]	OAIC guidance

Field	Content	Required by
Cause and circumstances	[Cyber attack, system fault, human error, theft or loss; any known cause]	OAIC guidance
Who has or may have obtained the information	[Known or likely parties]	OAIC guidance
Number of individuals affected (or estimate)	[number]	OAIC form
Containment and remediation steps taken	[Actions taken and planned]	OAIC guidance
How and when individuals are being notified (option 1, 2 or 3)	[Method and dates]	OAIC form
Other regulators and agencies notified	[APRA, ASIC, ASD, police, overseas regulators]	Good practice

Appendix D. Customer notice template

Adapt to the breach and channel. Include all the statement's contents (s26WL). Keep it short, plain and practical.

Section	Suggested wording
Subject / heading	Important information about your personal information
What happened	On [date], we found that [plain description of what happened]. It happened between [dates].
What information was involved	The information involved includes your [list the kinds of information that apply to this customer]. Your [passwords / card PINs] were not involved.
What we have done	We have [contained the breach / secured our systems / reported the matter to the OAIC, police and other authorities]. [We have added extra security checks to your account.]
What you should do	We recommend you: [specific steps, for example change your password; replace your driver licence; ask credit reporting bodies for a free ban period if you think you may be a victim of fraud; be alert to calls, emails or texts that claim to be from us].

Section	Suggested wording
How we can help	[Dedicated line, hours, web page; any credit monitoring, document replacement or identity support offered and how to take it up; support for customers in vulnerable circumstances; interpreter service.]
Scam warning	We will never ask you to click a link to log in, or to give us your password, a one-time code or a copy of your identity documents in response to this notice. If you are unsure whether a message is from us, call us on [known number] .
Who we are and how to contact us	[Organisation legal name, contact details] .
Complaints	If you are not happy with how we have handled this, contact us at [complaints contact] . You can also contact the Australian Financial Complaints Authority (AFCA) or the Office of the Australian Information Commissioner (OAIC).

Appendix E. Breach register fields

Field	Detail
Reference; linked incident register ID	Unique IDs
Dates	Occurred; aware of grounds for suspicion; 30-day deadline; contained; assessment completed; OAIC notified; individuals notified (first and last); closed
Description and cause	What happened; root cause category; cyber incident (yes / no)
Entity role and information type	APP entity, credit provider, credit reporting body, TFN recipient, CDR; kinds of information; sensitive information (yes / no)
Systems, business units and service providers involved	Names
Individuals	Number affected; number at risk; vulnerable individuals; jurisdictions
Rating	Critical, High, Medium or Low under the Incident & Issues Management Standard
Serious harm assessment	Outcome; link to Appendix B worksheet; remedial action and evidence
Eligible data breach decision	Yes / No; decision maker; reasons; exception relied on
Notification	OAIC reference; option used (1, 2, 3); method; number of notices sent and delivered
Other notifications	APRA, ASIC, ASD, police, AUSTRAC, overseas regulators, insurers, partners: decision, date and reference for each
Customer support	Support offered and take-up; complaints received; compensation paid
Eligible data breach declaration	Any declaration under s26X that applies, and how it was used
Costs	Response, legal, forensic, customer support, remediation, recoveries (insurance)

Field	Detail
Review and actions	Post-breach review date; issues and actions raised; owners and due dates; status
Closure	Closure date, approver and evidence



[Risk Taxonomy](#) [Operations](#) [Library](#) [Obligations Register](#) [Why a standard](#) [About](#)

Disclaimer

© 2026 Risk Frameworks Australia

Free general information only, provided free of charge. Not legal, financial or other professional advice, and used at your own risk. [Read the full disclaimer.](#)