

Data Breach Privacy Complaint Template

A general Australian privacy complaint template for customers whose personal information may have been exposed or mishandled

Important: This template provides general information only and is not legal advice. Edit it so that every statement accurately reflects your own circumstances. Do not exaggerate losses, make allegations you cannot support, or include passwords, complete banking details or unnecessary identity documents in an ordinary email.

How to Use This Template

Replace all text shown in square brackets with information that accurately reflects your own circumstances.

Delete any questions or requested outcomes that do not apply to you. Keep your complaint factual, clear and respectful.

Before sending it, check that:

- every statement is true and can be supported;
- dates, account references and contact details are correct;
- any financial loss or personal impact is described accurately;
- you have not included passwords, complete bank or card details, or unnecessary identity documents; and
- you have saved a copy of the complaint and any attachments.

Send the complaint to the organisation's privacy officer, complaints team or other official contact point. Ask for written confirmation that it has been recorded as a formal privacy complaint and request a complaint reference number.

Formal Privacy Complaint

To: [Organisation name / Privacy Officer / Complaints Team]

Email: [Official complaint email]

Date: [Date]

Subject: Formal Privacy Complaint – [Name of data breach or incident]

Dear [Privacy Officer / Complaints Team],

Please treat this letter as a formal privacy complaint and provide me with a complaint reference number.

I am writing regarding the data security incident notified to me on **[date notification received]** by **[organisation name]**.

Based on the information currently available, I understand that my personal information may have been accessed, disclosed, lost or otherwise compromised. I am concerned about the way my information was protected, the risks now created for me, and the time and effort I may need to spend protecting my identity, accounts and finances.

Please provide a clear written response addressing the questions set out below.

Information I Am Requesting

Please provide clear written answers to the following questions:

1. What personal information of mine was involved?
Please identify the specific categories of information affected, rather than providing only a general list of information that may have been exposed.
2. What happened to my information?
Please confirm whether it was accessed, viewed, copied, downloaded, disclosed, altered, published or otherwise obtained by an unauthorised person.
3. When did the incident occur?
Please provide the known or estimated date range during which my information may have been at risk.
4. When did your organisation first become aware of the incident?
5. When did your organisation first determine that my personal information may have been affected?
6. Why was I notified on the date stated above?
Please explain any delay between discovering the incident and notifying me.
7. Was my information encrypted or otherwise protected at the time of the incident?
8. Has my information been recovered, deleted or removed from any unauthorised location?
If this is not known, please state that clearly.
9. Is there evidence that my information has been misused, sold, published or used in attempted fraud or identity theft?
10. What steps have been taken to contain the incident and prevent a similar breach from occurring again?

11. Which regulators, law-enforcement bodies, credit-reporting bodies or other relevant agencies have been notified?

12. What support is available to me?

Please include any identity-monitoring services, specialist assistance, reimbursement process, account protections or other remedies being offered.

Impact on Me

Edit this section so that it accurately reflects your own circumstances. Delete any examples that do not apply.

As a result of this incident, I have experienced or may reasonably experience the following:

- concern about possible identity theft, fraud or misuse of my personal information;
- increased risk from scam calls, emails or text messages that may use genuine details to appear convincing;
- time spent changing passwords, securing accounts, contacting financial institutions or reviewing credit information;
- costs associated with replacing documents, obtaining professional assistance or protecting my identity;
- unauthorised transactions, attempted fraud or suspicious activity;
- disruption to my work, household or personal responsibilities;
- distress, anxiety or loss of confidence in the organisation's handling of my information; and
- other impacts described below.

Details of the impact on me:

[Describe what has actually happened. Include dates, amounts, reference numbers and supporting evidence where relevant.]

[Examples: suspicious calls received, accounts secured, hours spent resolving the matter, expenses incurred, fraudulent transactions, documents replaced or significant personal disruption.]

I have kept, or will keep, copies of relevant correspondence, receipts, screenshots, bank records and complaint reference numbers.

Outcome I Am Seeking

I ask that your organisation provide an appropriate response to this complaint, including the following where relevant:

1. **A clear written explanation** of what occurred, what information of mine was affected, and the steps taken in response.
2. **Confirmation of the protections now in place** to reduce the risk of further unauthorised access or misuse.
3. **Access to any support services being offered**, including identity monitoring, specialist identity-support services or account protections.
4. **Reimbursement of reasonable costs directly connected to the incident**, where supported by receipts or other evidence.
5. **Consideration of an appropriate remedy** for any financial loss, non-financial harm, distress, inconvenience or disruption I can substantiate.
6. **Correction, deletion or restriction of affected information**, where appropriate and legally available.
7. **Written confirmation that this matter has been recorded as a formal privacy complaint**, together with a complaint reference number.
8. **A substantive written response within 30 days**, or an explanation if additional time is required.

Delete any requested outcome that does not apply to your circumstances. Do not request compensation or reimbursement for losses or costs you have not actually experienced or cannot reasonably support.

Supporting Documents

I have attached, or can provide if requested, copies of documents relevant to this complaint, including:

- the organisation's data breach notification;
- later updates or correspondence about the incident;
- screenshots of suspicious emails, text messages or account activity;
- bank or card records showing unauthorised or suspicious transactions;
- receipts for reasonable expenses connected to the incident;
- records of calls, complaint reference numbers and dates of contact;
- evidence of identity-document replacement or credit-monitoring costs; and
- any other material supporting the impact described above.

Attach only documents that are relevant and necessary. Keep copies of everything you send.

Do not send passwords, complete banking or card details, security codes or unnecessary copies of identity documents by ordinary email. Where sensitive verification is required, ask the organisation to provide a secure method.

Closing and Escalation

Please confirm in writing that this complaint has been formally recorded and provide me with:

- a complaint reference number;
- the name or department responsible for reviewing it; and
- the expected timeframe for a substantive response.

I would appreciate a written response within 30 days.

If I do not receive a response within that period, or if the matter is not resolved satisfactorily, I may refer the complaint to the Office of the Australian Information Commissioner or another relevant external dispute-resolution body.

I reserve the right to provide further information if additional impacts, costs or suspicious activity arise.

Thank you for your attention to this matter.

Yours sincerely,

[Full name]

[Customer or account number]

[Email address]

[Telephone number]

Before sending, replace every bracketed field, remove instructions and delete anything that does not accurately apply to your circumstances.