|  |
| --- |
| **How to use this template**  This template aims to assist organisations when notifying affected individuals about a data breach. It should be read in conjunction with OVIC’s guide on [‘Managing the privacy impacts of a data breach.’](https://ovic.vic.gov.au/book/managing-the-privacy-impacts-of-a-data-breach/#When_to_notify)  The content of each notification will depend on the circumstances. Organisations should not simply stick to the content of this template. They should decide to change and add further information as required – such as by expressing their regret or apologies in whatever way they feel is appropriate.  Words highlighted in yellow are recommended whilst words highlighted in green provide additional drafting information and should be omitted from the final version. |

[Affected individual’s name]

[Affected individual’s address]

[Date]

**Notification of privacy incident**

Dear [affected individual’s name],

We are writing to let you know about a recent privacy breach that involved some of your personal information. This letter will explain what happened, how we have responded and what it means for you.

**What happened?**

[On/between] [date/time period], [provide a summary of the incident, why it constitutes a breach and steps you have taken to investigate what happened]

This section should be detailed so the person has a good understanding of what occurred and why what occurred is considered a privacy breach. The language should be clear and tailored such that a layperson with no technical experience can understand the nature of the breach.

It is often helpful to use the active rather than passive voice. You should also be as specific as possible e.g. instead of referring to a ‘third party’ you may wish to identify the third party or at least describe the type of third party.

**What information was affected?**

Based on our investigation, we understand that your personal information that has been affected by this incident includes:

* [List the personal information affected].

Examples of personal information include: name, residential address, birth date, phone number, credit card number or the fact the individual made a complaint to the organisation.

Where the personal information is complex or numerous, organisations should consider providing affected individuals with an extract of the affected personal information in an appendix to the notification letter.

Details about the personal information involved will allow affected individuals to make their own assessment about the likely harm that they may experience because of the incident and develop proactive steps to protect themselves.

**What have we done in response to the breach?**

[Describe the steps you have taken or are intending to take to contain the breach and minimise any potential harm.]

[Describe the steps you have taken or are intending to take to reduce the likelihood of similar incidents occurring in the future.]

This information may help an affected individual feel reassured about your organisation’s response and information handling practices; reduce any distress they initially experienced; and impact their own risk assessment.  
 **What does this mean for you?**

You should carefully review the information that was affected by this incident and think about whether this could result in you experiencing any harm. Some of the steps you may consider taking to protect yourself include:

[Example - Where the risk of harm is identity fraud]

* Be aware of emails and telephone calls from people requesting your personal details, (especially things like your date of birth, residential address, email address, username or passwords which are often used to verify your identity).
* Change your account password.
* Contact IDCare on **1300 432 273** or visit [**www.idcare.org**](http://www.idcare.org) who can provide you with additional guidance on the steps you can take to protect yourself from identity fraud.

[Example - Where the risk of harm is spam]

* If you start to receive unwanted telemarketing calls, consider registering your number with the Australian Communications and Media Authority’s ‘Do Not Call register’ by visiting [**www.donotcall.gov.au/consumers/register-your-numbers**](http://www.donotcall.gov.au/consumers/register-your-numbers). You can also contact your service provider and request to change your number.

[Example - Where the risk of harm involves financial information]

* Alert your financial institution so that they can implement additional monitoring and security protocols on your account.
* Closely monitor your financial statements for unauthorised transactions. If you identify a transaction you didn’t make, report it immediately to your financial institution.
* Change your online bank account password, banking PIN and enable multi-factor authentication if possible.
* Contact Australia’s three credit reporting agencies (Equifax, illion and Experian) to confirm if your identity has been used to obtain credit without your knowledge or to request for a credit ban to be put in place.

[Where the information affected includes TFN or superannuation details]

* Contact the Australian Tax Office on **1800 467 033** or your superannuation fund so that they can consider placing additional monitoring and security protocols on your account.

Further information is also available on the Office of the Victorian Information Commissioner’s website at [**www.ovic.vic.gov.au/privacy/for-the-public/data-breaches-and-you**](http://www.ovic.vic.gov.au/privacy/for-the-public/data-breaches-and-you)**.**

**More information and making a complaint**

If you have any concerns about what has happened or would like further information, you can contact:

[individual or department’s name within your organisation]

[phone number] or [email].

If you are not satisfied with how we have handled this incident or you have experienced some harm as a result, you can make a privacy complaint. You can do so by contacting us by email at [email].

It would be helpful if you could explain how you have been affected by the breach and what you would like us to do to resolve your complaint.

If we cannot resolve your complaint, you can then make a complaint to the Office of the Victorian Information Commissioner (**OVIC**). You can find out more about how to make a complaint to OVIC at <https://ovic.vic.gov.au/privacy/for-the-public/complaints/>.

Yours sincerely,

[Name of representative]

[Position of representative]

[Organisation name]