How to respond if you get a data breach notification

If you have received a data breach notification, it is natural to feel distressed and confused about what you should do.

This resource explains what a data breach is, how you can reduce the risk of suffering harm as a result of a data breach, what actions you can take and when to make a privacy complaint.

What is a data breach?

A **data breach** occurs when your personal information that is held by an organisation is accessed or disclosed in a way that it shouldn't have been (e.g. where it is lost, stolen, or given to the wrong person).

Data breaches have the potential to cause you harm including financial, physical or emotional harm. If you are notified of a data breach, you should act quickly to reduce your chances of experiencing harm.

How to reduce your risk of harm

You should first identify what information has been affected and think about what harm this could lead to. To find out what information has been affected read the data breach notification closely or contact the organisation that notified you of the breach and ask for more information.

This will help you determine what steps you can take depending on the information involved.

When a breach involves identity and contact information

Identity and contact information includes your photograph, full name, date of birth, driver's license, passport numbers, phone number, email address and residential address.

If your identity and contact information is disclosed to third parties, there is a risk of identity theft and third parties being able to locate or contact you.

If your identity or contact information is affected by a data breach, some actions you can take include:

- contact Victoria Police on **13 14 44** if you are concerned about your physical safety**.** If you have immediate safety concerns, call **000**;
- if you receive unwanted telemarketing calls, register your number with the Australian Communications and Media Authority **'Do Not Call register'** by visiting **www.donotcall.gov.au/consumers/register-your-numbers.** You can also contact your service provider and request to change your number;
- if you experience online bullying or harassment, visit the Office of the eSafety Commissioner at **www.esafety.gov.au.** For more tips about staying safe online, visit Stay Smart Online at **www.staysmartonline.gov.au**; and
- to assist with any mental or emotional distress, contact your General Practitioner, Beyond Blue on **1300 24 636** or Lifeline on **13 11 14.**

If you become a victim of identity theft or fraud following a data breach, some actions you can take include:

- change your online account passwords and be wary of scam emails. Find out more at **www.scamwatch.gov.au**;
- contact IDCare on **1300 432 273** or visit **www.idcare.org**. IDCare operates a free service for identity support and can help you develop an action plan;

- limit the personal information you share online. For example, information like your mother's maiden name or the car you drive is sometimes used by service providers and financial institutions as security questions to identify individuals;

- contact the Australian Passport Office on **13 12 32** if your passport has been affected; and

- contact VicRoads on **13 11 71** if your Victorian driver's licence has been affected. It is important to note that a Victorian driver's licence number can only be changed where you can show that a criminal use of your driver's licence has occurred.

When a breach involves financial information

Financial information includes your credit card details, online banking credentials, superannuation details and Tax File Number.

If a data breach involves your financial information being disclosed to third parties, risks include fraudulent transactions and attempts to access your money or assets.

If your financial information is affected by a data breach, some actions you can take include:

- alert your financial institution so that they can implement additional monitoring and security controls;

- closely monitor your financial transactions and if you identify a transaction you didn't make, report it immediately to your financial institution;

- if your online banking credentials are affected, 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 and put a Credit Ban in place; and

- if your Tax File Number or superannuation details are affected, contact the Australian Tax Office (**ATO**) on **1800 467 033** or your superannuation fund so that they can consider placing additional security controls on your accounts.

Making a privacy complaint

If you have already experienced harm as a result of a data breach and want to make a privacy complaint, you can:

- contact the organisation responsible for the breach, explain the harm you have experienced and discuss potential solutions;

- if you are dissatisfied with the organisation's response, you can pursue a privacy complaint by contacting OVIC (where the organisation is a Victorian public sector organisation) or the Office of the Australian Information Commissioner (where the organisation is a Commonwealth agency or private organisation).

Further Information

For more information, contact OVIC:

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au