Australian Government
Office of the Australian Information Commissioner

Preparing for the Notifiable Data Breaches scheme

Guidance from the Office of the Australian Information Commissioner

Presented by Annan Boag and Sophie Higgins

OAIC

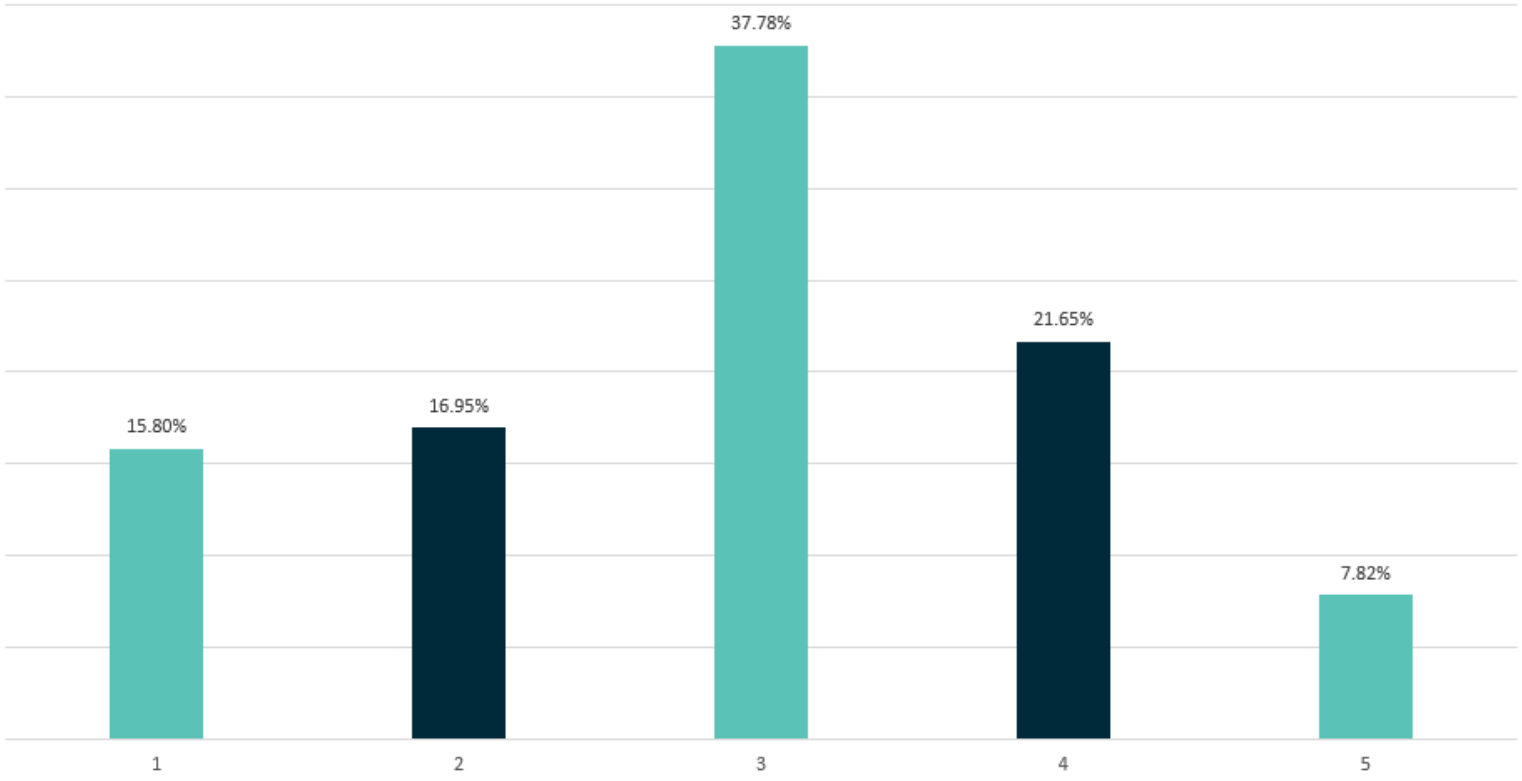
Welcome to the webinar

What we will cover today:

- Background on the Notifiable Data Breaches (NDB) scheme
- Who needs to comply with the NDB scheme?
- What is an ‘eligible data breach’?
- What is remedial action?
- When to conduct an assessment of a suspected data breach
- How to notify affected individuals and the Australian Information Commissioner
- Exceptions to the notification requirements
- Your questions.

Level of NDB scheme knowledge for webinar participants

- 1 – Little/no understanding. 5 – High level of understanding.



Background on the NDB scheme

- The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the NDB scheme in Australia (to be Part IIIC of the *Privacy Act 1988* on commencement)

- The NDB scheme sets out obligations for notifying affected individuals, and the Australian Information Commissioner, about a data breach which is likely to result in serious harm

- The NDB scheme strengthens protections to personal information — providing affected individuals with an opportunity to take steps to protect their personal information following a breach. Further, the transparency supported by the scheme encourages greater personal information security capability across Australian industries

- Over time, this transparency builds consumer and community confidence in the handling of personal information.

Australian Government
Office of the Australian Information Commissioner

Who needs to comply with the NDB scheme?

Your questions:

Do companies outside Australia have to comply with the Notifiable Data Breaches (NDB) scheme?

Does the NDB scheme effect all education providers?

Will the NDB scheme apply to business with a turn over of less than 3 million?

What are the responsibilities of third party service providers?

How does the NDB scheme impact a university?

Does the NDB scheme apply to unauthorised access to employee records?

The NDB scheme applies to organisations with obligations under the *Privacy Act 1988*

- Australian Government agencies
- All businesses and not-for-profit organisations with an annual turnover of $3 million or more
- Some small business operators, including:
  - All private sector health service providers
  - Those that trade in personal information
  - TFN recipients (if annual turnover is below $3 million, the NDB scheme will apply only in relation to TFN information)
  - Those that hold personal information in relation to certain activities, for example; providing services to the Commonwealth under a contract.

Australian Government
Office of the Australian Information Commissioner

What is an eligible data breach?

Your questions:

How do you decide what is serious? What may be serious for one person may not be serious for someone else?

What constitutes 'serious harm'?

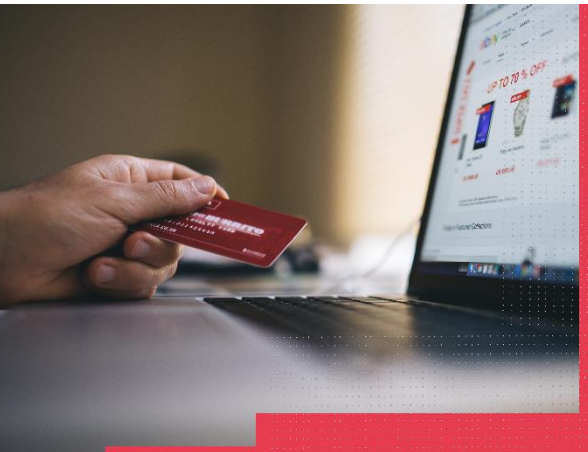
Any advice on, or a clearer definition of serious harm?

Case study

Poll: Consider the case study and provide your answer. Do you have to notify?

You work for a business operating a chain of stores throughout Australia. Your annual turnover is over $3 million. About 3,000 of your customers have joined your website so that they can make online purchases.

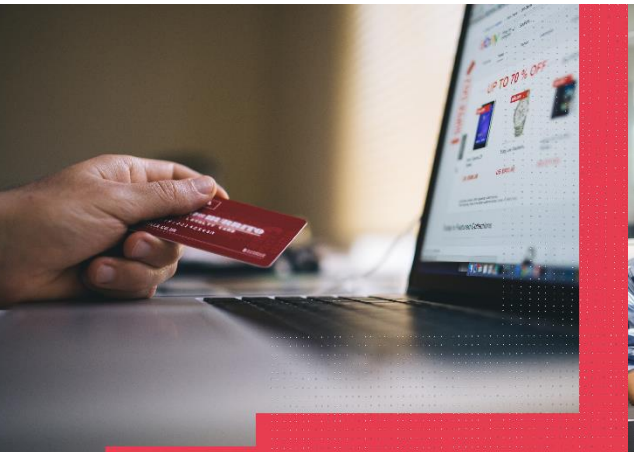
An attacker, exploiting an unpatched vulnerability in your customer relationship management (CRM) system, gains access to the customer database for your online store, which includes customer purchase histories and contact details.



Case study

Your IT security team notices this, and is able to block further access. A day later you are contacted by two customers who say they have received emails from your company requesting their credit card details to confirm a recent purchase. Your company would never request credit card details by email.

Do you need to notify your customers and the Australian Information Commissioner of the data breach?



‘Eligible data breaches’ under the NDB scheme

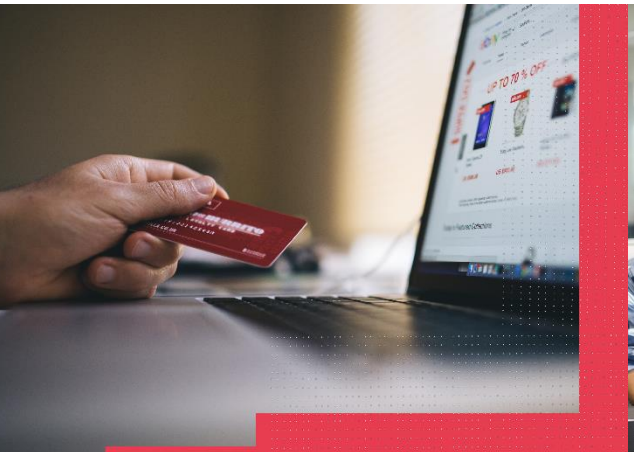
- An eligible data breach occurs when three criteria are met:
  - There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
  - This is likely to result in serious harm to one or more individuals, and
  - The entity has not been able to prevent the likely risk of serious harm with remedial action.
- ‘Serious harm’ can be psychological, emotional, physical, reputational, or other forms of harm
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

Case study

Consider…

1. The type or types of personal information involved in the data breach.
2. The circumstances of the data breach.
3. The nature of the harm that may result from the data breach.

See the full list of factors in s 26WG.



Remedial action

- If you take remedial action that prevents the likelihood of serious harm occurring, then the breach is not an eligible data breach

- For breaches where personal information is lost, the remedial action is adequate if it prevents the unauthorised access or disclosure of personal information.

Examples of remedial action

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside the entity. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The sender then confirms that the recipient has not copied, and has permanently deleted the data file.

An employee leaves a smartphone on public transport while on their way to work. When the employee arrives at work they realise that the smartphone has been lost, and ask their employer's IT support staff to remotely delete the information on the smartphone. Because of the security measures on the smartphone, the IT support staff are confident that its content could not have been accessed in the short period between when it was lost and when its contents were deleted.

Australian Government
Office of the Australian Information Commissioner

When to conduct an assessment of a suspected data breach

Your questions:

There is sometimes no evidence that the data has been subject to unauthorised access, but at the same time it cannot be proven that there has been no access.

How does a company evaluate its notification obligations where there is no evidence of serious harm and no evidence of access or likelihood of harm?

If you suspect a data breach which may meet the threshold of ‘likely to result in serious harm’, you must conduct an assessment

- Generally, there is a maximum of 30 days to conduct this assessment. This begins from when you become aware of a potential breach
- Ahead of the NDB scheme, you should review your data breach response framework to ensure relevant personnel will be made aware of a breach as soon as practicable
- It is not expected that every data breach will require an assessment that takes 30 days to complete before notification occurs. You must notify as soon as practicable once you hold the belief an eligible data breach has occurred.

What is involved in an assessment

- The Act says assessments must be ‘reasonable’ and ‘expeditious’
- It is up to entities to decide what process to follow when conducting an assessment
- Generally, we suggest that an assessment should cover off the following three stages:

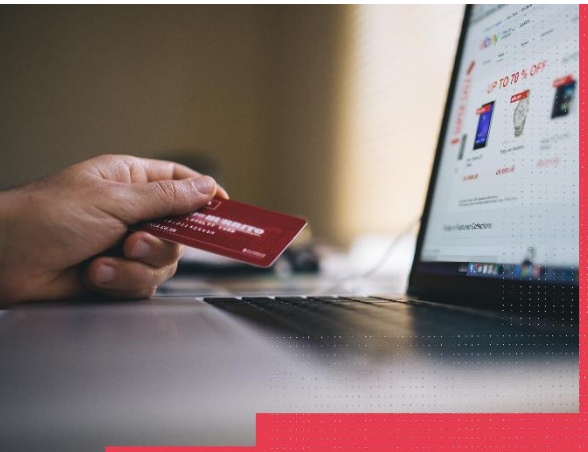
1. **Initiate:** decide whether an assessment is necessary and identify which person or group will be responsible for completing it
2. **Investigate:** quickly gather relevant information about the suspected breach, including, for example, what personal information is affected, who may have had access to the information and the likely impacts, and
3. **Evaluate**: make a decision, based on the investigation, about whether the identified breach is an eligible data breach.

Case study

You own a pharmacy. Your IT provider calls you to tell you that there has been an unusual access to your customer database overnight. It appears that one of your casual employees, who usually only works in store during the day, logged onto the database at 2:00 am. You call the employee and they say it wasn't them. They mention that their password is '123456'. Maybe somebody guessed it?

Discussion:

- Does the organisation need to conduct an assessment?
- When does the clock start on the 30 days to conduct the assessment?
- What do you do now?

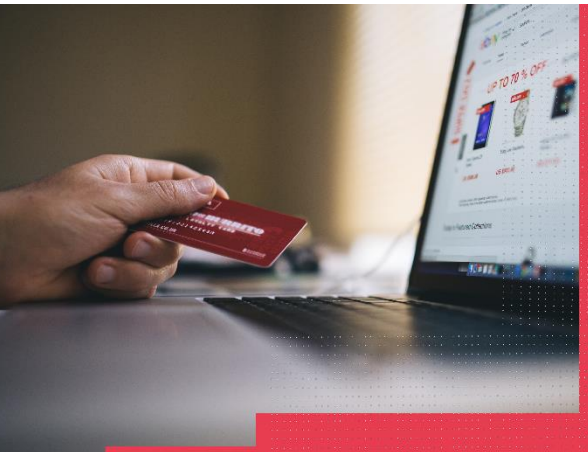


Case study

Poll: Consider the below information and provide your answer. Do you think this is a notifiable data breach?

During the course of the assessment, it is established that:

- The customer database was accessed by someone outside the organisation
- That person accessed the purchase history for two people who may be members of the same family (they live in the same suburb and share a last name)
- The information accessed included records of prescription drugs for treatment of mental illness, which had been dispensed to those people.



Australian Government
Office of the Australian Information Commissioner

How to notify

Your questions:

What format should the notification look like?

Who is ultimately responsible for the notification of a data breach, particularly if there are a number of suppliers and/or clients involved in the project?

How should organisations advise the OAIC (is there an email address, post-box etc. we should be using)?

Who to notify

You must notify any individuals that are at likely risk of serious harm as a result of a data breach. You must also notify the Australian Information Commissioner.

Notifying affected individuals

There are three options for notification:

- Notify all individuals whose personal information is involved in the eligible data breach
- Notify only the individuals who are at likely risk of serious harm; or
- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm.

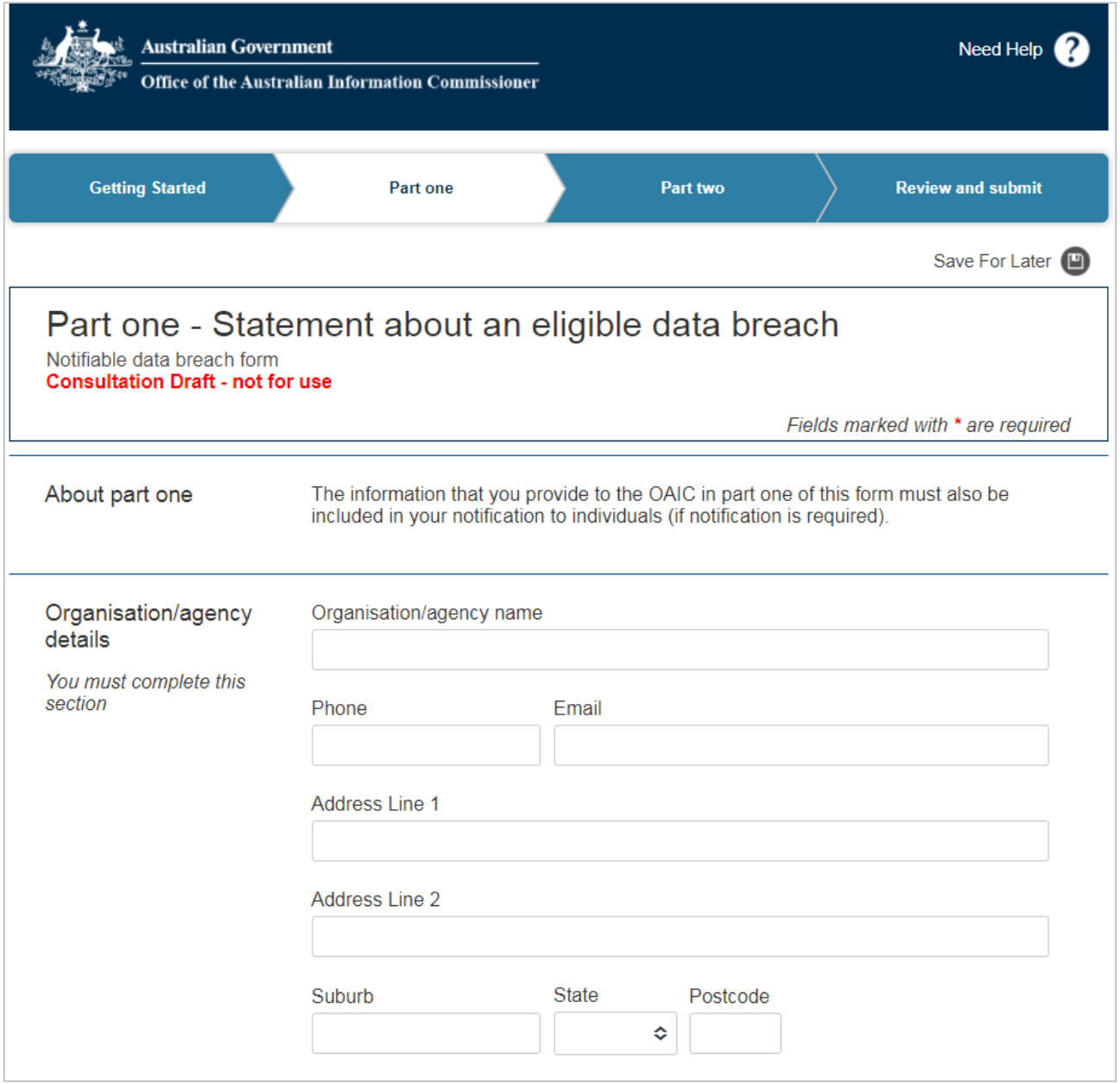
There is flexibility in the way you notify individuals.

What to include in a statement to the Australian Information Commissioner

Your notification to the Australian Information Commissioner must be in the form of a statement, which includes the following information:

- The identity and contact details of you agency/organisation
- A description of the eligible data breach
- The kind or kinds of information involved in the eligible data breach
- What steps your agency/organisation recommends that individuals take in response to the eligible data breach.

This statement must be provided to the Commissioner as soon as practicable. We will have an electronic form we would like used for this purpose.


Australian Government
Office of the Australian Information Commissioner
Need Help
Getting Started
Part one
Part two
Review and submit
Save For Later
Part one - Statement about an eligible data breach
Notifiable data breach form
Consultation Draft - not for use
Fields marked with * are required
About part one
The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required).
Organisation/agency details
You must complete this section
Organisation/agency name
Phone
Email
Address Line 1
Address Line 2
Suburb
State
Postcode

Australian Government
Office of the Australian Information Commissioner

Exceptions to the notification requirements

Exceptions apply in limited circumstances

- There are some exceptions to notification requirements, which relate to:
  - Eligible data breaches of other entities (s 26WJ)
  - Enforcement related activities (s 26WN)
  - Inconsistency with secrecy provisions (s 26WP)
  - Declaration by the Australian Information Commissioner (s 26WQ)
  - My Health Record data breaches (s 26WD).

Australian Government
Office of the Australian Information Commissioner

Summary

Maintain personal information security (APP 11)

APP entities must take reasonable steps to protect personal information they hold.

Possible data breach occurs

Contain

As your first priority, take immediate steps to contain the possible data breach.

Assess

Consider whether the breach is likely to result in serious harm for any of the individuals whose information is involved.

If you have reasonable grounds to believe there is an eligible breach, you must notify. If you only have reasonable grounds to suspect an eligible breach, you must conduct a reasonable and expeditious assessment of whether there is a notifiable breach, usually within 30 days (26WH).

Take remedial action

Where possible, an entity should take steps to reduce the likelihood of harm to affected individuals caused by the breach. This might involve recovering the information, or providing assistance to affected individuals.

If remedial action is able to make serious harm not likely, then notification is not required, and entities can proceed directly to 'Review' (26WF).

Notify

Where serious harm to affected individuals is likely, the entity must notify those individuals and the Commissioner (26WK; 26WL). The notification must contain the entity's contact details, a description of the breach, the kind/s of information concerned, and recommended steps for individuals. It may contain other information.

If practicable, notify those individuals at likely risk of serious harm directly. If it is not practicable to notify directly, you can publish a statement on your website, and take steps to draw it to the attention of the relevant individuals.

In certain circumstances, an exception may apply meaning notification is not required (26WM – 26WQ)

Review

Consider how the breach occurred and whether to enhance your personal information security measures.

OAIC

Australian Government
Office of the Australian Information Commissioner

What to do next

Visit: www.oaic.gov.au/ndb

Q&A

oaic.gov.au