Australian Government
Office of the Australian Information Commissioner

Notifiable Data Breach Form

About this form

Notifiable Data Breach statement

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the Privacy Act 1988.

Part one is the 'statement' about a data breach required by section 26WK of the Privacy Act. If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

The OAIC encourages entities to voluntarily provide additional information about the eligible data breach in part two of this form. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

Before completing this form, we recommend that you read our resource *What to include in an eligible data breach statement*.

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review the *Identifying eligible data breaches* resource.

The OAIC will send an acknowledgement of your statement about an eligible data breach on receipt with a reference number.

You can save this form at any point and return to complete it within 3 days. To save your form, click on the Save For Later button on the top right-hand corner of this form. If you do not submit your saved form within 3 days, your saved information will be permanently erased.

Refreshing your browser will clear any information that you have not saved. If you need to refresh your browser while completing this form and wish to keep your changes, please save the form first.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles.

We collect this information to consider and respond to your breach notification. We may use it to contact you.

More information about how the OAIC handles personal information is available in our privacy policy.

Part one - Statement about an eligible data breach

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 *

Consumer Credit Legal Service (WA) Inc

Phone *

[redacted]

Email *

[redacted]

Address Line 1 *

Level 1, 231 Adelaide Terrace

Address Line 2

Suburb *

Perth

State *

WA

Postcode *

6000

Other contact details

Description of the eligible data breach

You must complete this section

A description of the eligible data breach: *

On the long weekend of 3 to 5 March 2018, unauthorised access of CCLSWA's MYOB program occurred.

On 6 March 2018 we noticed that the administrator account had been logged into the program over the weekend, but there was no report of transactions.
We became aware of the unauthorised access on 8 March 2018 when we were notified by staff that they had not received their fortnightly payment. It was then we compared the current bank details on MYOB to a backed up version and realised that they had been changed. At this point in time, we changed the administrator account's password. However, on 12 March 2018 there was a further unauthorised access, in which an unauthorised user managed to log in using the administrator's password on the second try and change that password. The unauthorised access was once again limited to changing the bank details on the MYOB program. We have taken steps since that time to prevent any further access and no further unauthorised access has occurred.

Information involved in the data breach

You must complete this section

Kind or kinds of personal information involved in the data breach: *

The bank account details of 6 employees were changed. However, by accessing the MYOB program, the unauthorised user had access to the following information of our 7 employees and 47 past employees:
(a) full names and contact information;
(b) dates of birth;
(c) payroll and leave history;
(d) bank account details;
(e) tax file numbers; and
(f) superannuation account details.
They did not access medical certificates as these are stored on a separate program which was not accessed.

In addition, please select any categories that apply:

- [x] Financial details
- [x] Tax File Number (TFN)
- [ ] Identity information (e.g. Centrelink Reference Number, passport number, driver license number)
- [x] Contact information (e.g. home address, phone number, email address)
- [ ] Health information
- [ ] Other sensitive information (e.g. sexual orientation, political or religious views)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach: *

We have notified our current employees and recommended that they take steps to reduce the risk that they experience serious harm as a result of this unauthorised access, including by contacting their bank, superannuation fund and the Australian Tax Office. We will also provide this notification to our former employees. Based on advice we have received, we also intend to notify present and past employees that they have the option of speaking with IDCARE, which we understand provides free and confidential support in respect of data breaches and disclosure of identifying information. We will also provide information on obtaining credit alerts from credit reporting bodies to present and past employees, and we will offer to reimburse the cost of this for one year, being $79.95.

Other entities affected

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation/agency affected?

- ( ) Yes
- (•) No

s 45

s 45

[redacted]

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach.

We have notified our current employees and recommended that they take steps to reduce the risk that they experience serious harm as a result of this unauthorised access, including by contacting their bank, superannuation fund and the Australian Tax Office. We will also provide this notification to our former employees. Based on advice we have received, we also intend to notify present and past employees that they have the option of speaking with IDCARE, which we understand provides free and confidential support in respect of data breaches and disclosure of identifying information. We will also provide information on obtaining credit alerts from credit reporting bodies to present and past employees, and we will offer to reimburse the cost of this for one year, being $79.95.

s 45

s 45

s 45