Our reference: FOIREQ22/00135

Attention: **Steven Roddis**

By Email: foi+request-8969-366bc574@righttoknow.org.au

Your Freedom of Information request – FOIREQ22/00135

Dear Mr Roddis,

I refer to your request for access to documents made under the *Freedom of Information Act* 1982 (Cth) (the FOI Act) received on 31 May 2022.

You seek access to:

> *... documents between OAIC and CTARS regarding the May 2022 Data Breach.*

On 3 June 2022, Matilda Grimm wrote to you to acknowledge receipt of your request.

On 14 June 2022, Matilda Grimm wrote to you to advise third party consultation was required and the new decision due date was 1 August 2022.

Decision

I am an officer authorised under s 23(1) of the FOI Act to make decisions in relation to FOI requests.

Searches were conducted by the Notifiable Data Breach team.

I have identified three documents within the scope of your request.

I have decided to give you access to one document in part, and refuse access to two documents.

Reasons for Decision

Material taken into account

In making my decision, I have had regard to the following:

- your freedom of information request dated 31 May 2022;
- the FOI Act, in particular sections 47E, 47G and 11A(5);

- the Guidelines issued by the Australian Information Commissioner under s 93A of the FOI Act (the FOI Guidelines), specifically paragraphs [6.7] – [6.28], [6.95] – [6.123] and [6.180] – [6.213];

- searches conducted and advice provided by the team responsible for notifiable data breaches;

- the documents at issue; and

- relevant case law.

Certain operations of agencies – s 47E(d)

I have decided that two documents are exempt in full and one document exempt in part under s 47E(d) of the FOI Act.

The documents I have found exempt under s 47E(d) are the Notifiable Data Breach Form submitted by CTARS Pty Ltd (CTARS), which contains details of the data breach, and an email from CTARS listing all affected clients. The other material which I have found exempt is the file reference number of the notifiable data breach matter.

Under s 47E(1)(d) of the FOI Act, a document is conditionally exempt if its disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of the operations of an agency.

The FOI Guidelines at [6.101] provide:

> *"For the grounds in ss 47E(a)–(d) to apply, the predicted effect needs to be reasonably expected to occur. The term 'could reasonably be expected' is explained in greater detail in Part 5. There must be more than merely an assumption or allegation that damage may occur if the document were to be released."*

Additionally, at [6.103] the FOI Guidelines further explain:

> *"An agency cannot merely assert that an effect would occur following disclosure. The particulars of the predicted effect should be identified during the decision making process, including whether the effect could reasonably be expected to occur. Where the conditional exemption is relied upon, the relevant particulars and reasons should form part of the decision maker's statement of reasons, if they can be included without disclosing exempt material (s 26, see Part 3)."*

Further, the FOI Guidelines provide (at [5.16] – [5.17]) that I must assess the likelihood of the predicted damage occurring after disclosure. However, there need not be certainty that the damage would occur.

Functions and powers of the OAIC

In order to determine whether disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of the operations of the OAIC, I have taken into consideration the functions and activities of the OAIC.

Due to the nature of the relevant material, I have had regard to:

- the Australian Information Commissioner's investigative powers under the *Privacy Act 1988* (Cth) (Privacy Act)
- the OAIC's Notifiable Data Breaches investigation processes

The OAIC is an independent statutory agency within the Attorney-General's portfolio, established under the *Australian Information Commissioner Act 2010* (Cth) (AIC Act). The OAIC comprises the Australian Information Commissioner and the Privacy Commissioner (both offices currently held by Angelene Falk), the FOI Commissioner (currently held by Leo Hardiman) and the staff of the OAIC.

The OAIC is established under s 5 of the AIC Act. Section 5 also provides that the Information Commissioner is the Head of the OAIC for the purposes of the *Public Service Act 1999* (Cth). Section 5 further provides that for the purposes of the *Public Governance, Performance and Accountability Act 2019* (Cth) the Information Commissioner is the accountable authority of the OAIC.

Under the AIC Act and the Privacy Act, the Information Commissioner has a range of functions and powers under the Notifiable Data Breaches scheme, including to:

- receive notifications of eligible data breaches;
- encourage compliance with the scheme, including by handling complaints, conducting investigations and taking other regulatory action;
- offer advice and guidance to regulated organisations; and
- provide information to the community about the operation of the NDB scheme.

I find it is likely that disclosure of the documents would decrease the willingness of organisations affected by data breaches to make full disclosure to the OAIC. If organisations impacted by a notifiable data breach believe their sensitive business information may be disclosed publicly, they will be less likely to provide the necessary information for the OAIC to conduct its Notifiable Data Breaches scheme functions. This will have a substantial adverse effect on the proper and efficient conduct of the OAIC as the body responsible for overseeing the Notifiable Data Breaches scheme.

The investigation into the CTARS data breach is currently ongoing, and the OAIC relies on CTARS to provide as much information as possible so the OAIC can consider whether further action is required. While organisations are required to report data breach incidents to the OAIC, the extent of information provided is voluntary. At a minimum, organisations must provide the following information:

- the organisation or agency's name and contact details;
- a description of the data breach;
- the kinds of information involved; and
- recommendations about the steps individuals should take in response to the data breach.

However, as noted on the OAIC's website,[1] the OAIC recommends reporting organisations provide the following information to assist the OAIC to fully investigate the breach:

- The circumstances of the data breach
- What the organisation has done to contain the data breach
- Whether any remedial action has been taken

The OAIC website also advises reporting organisations that "…The more information you tell us about the circumstances of the data breach, what you've done to contain the data breach and any remedial action you've taken, will help us respond to your notification". The OAIC relies on the information provided by the organisations in order to consider whether further regulation action, if any, is required.

In these circumstances, based on the information before me at this time, I am satisfied that the disclosure of the relevant documents in a notification data breach reported to the OAIC at this time, where the FOI applicant is not the reporting organisation, would, or could be reasonably expected to have a substantial adverse effect on the proper and efficient operations of the OAIC in investigating notifiable data breaches.

For these reasons, I am satisfied that the relevant information is conditionally exempt.

Business affairs exemption – s 47G

I have also decided that the two documents which I have found exempt under s 47E(d),[2] are alternatively exempt under s 47G(1)(a) and s 47G(1)(b).

Under s 47G(1) of the FOI Act, a document is conditionally exempt from disclosure if its release would disclose information concerning the business, commercial or financial affairs of an organisation or undertaking, in circumstances where disclosure of such information would unreasonably affect an organisation in the undertaking of its lawful business or commercial affairs. As noted in *Seven Network Operations Limited and Australian Human Rights Commission* [2021] AICmr 66 [156-157]:

> *"… the business information exemption is intended to protect the interests of third parties dealing with the government. The operation of s 47G depends on the effect of disclosure rather than the precise nature of the information itself. Notwithstanding this, the information must have some relevance to a person in respect of their business or professional affairs or to the business, commercial and financial affairs of the*

[1] Report a data breach - Home (oaic.gov.au)

[2] Documents 1 and 3.

organisation… The term 'business affairs' has been interpreted to mean 'the totality of the money-making affairs of an organisation or undertaking as distinct from its private or internal affairs'."

In this instance, the exempt documents contain information about the type of software used, the cause of the data breach and a list of CTARS' clients, which relate to the business affairs of CTARS. The information specifically relates to CTARS' money-making affairs since it outlines details of CTARS' client list and cloud-based client management system, which it provides to organisations providing care under the National Disability Insurance Scheme (NDIS) and children in Out of Home Care (OOHC).

I am therefore satisfied that this is information concerning the business affairs of CTARS.

Unreasonable adverse effect – s 47G(1)(a)

In order for s 47G(1)(a) to apply, disclosure must unreasonably affect the organisation to which the information relates. As explained by the FOI Guidelines at [6.187-6.188]:

"The presence of 'unreasonably' in s 47G(1) implies a need to balance public and private interests. The public interest, or some aspect of it, will be one of the factors in determining whether the adverse effect of disclosure on a person in respect of his or her business affairs is unreasonable. A decision maker must balance the public and private interest factors to decide whether disclosure is unreasonable for the purposes of s 47G(1)(a); but this does not amount to the public interest test of s 11A(5) which follows later in the decision process ...

The test of reasonableness applies not to the claim of harm but to the objective assessment of the expected adverse effect. For example, the disclosure of information that a business' activities pose a threat to public safety, damage the natural environment; or that a service provider has made false claims for government money may have a substantial adverse effect on that business but may be reasonable in the circumstances to disclose. Similarly, it would not be unreasonable to disclose information about a business that revealed serious criminality. These considerations require a weighing of a public interest against a private interest, preserving the profitability of a business, but at this stage it bears only on the threshold question of whether the disclosure would be unreasonable."

In *Bell and Secretary, Department of Health (Freedom of information)* [2015] AATA 494, Deputy President Forgie explained at [48]:

"Returning to s 47G(1)(a), it seems to me that the addition of a public interest test in s 11A(5) makes no difference to the continuing relevance of public interest when interpreting s 47G(1)(a). The public interest, or some aspect of it, will be one of the factors in determining whether the adverse effect of disclosure on a person in respect of his or her business affairs is unreasonable. It will be balanced against factors that may not be regarded as aspects of the public interest but as aspects relevant only to the interests of the person whose interests might be affected by disclosure. The

outcome of balancing all of the relevant factors –public interest or otherwise – will resolve the issue of whether disclosure of a document under the FOI Act would, or could reasonably be expected to, unreasonably affect that person adversely in respect of his or her business affairs or have another adverse effect described in s 47G(1)(a).”

In this instance, I am satisfied that disclosure of CTARS' business information, and the adverse effect that this disclosure would have, would be unreasonable. I am satisfied that this is commercially sensitive information, and that disclosure of this information could give CTARS' competitors an unfair commercial advantage, through revealing to other parties details of CTARS' software and security measures, and its client list. In addition, information detailing CTARS' security measures and how a third party accessed the software could further compromise the security of its systems. In my view, disclosure of this material is likely to unreasonably affect CTARS' business affairs.

In these circumstances, I am satisfied that disclosure of these documents at this time would, or could reasonably be expected to, unreasonably adversely affect CTARS in respect of its lawful business affairs (s 47G(1)(a)).

Prejudice future supply of information – s 47G(1)(b)

In addition to s 47G(1)(a), s 47G(1)(b) applies where disclosure could reasonably be expected to prejudice the future supply of information to the OAIC for the purpose of the administration of matters administered by the OAIC. The FOI Guidelines provide, at [6.198]:

“This limb of the conditional exemption comprises two parts:

- *a reasonable expectation of a reduction in the quantity or quality of business affairs information to the government*
- *the reduction will prejudice the operations of the agency”*

The FOI Guidelines further provide, at [6.200] – [6.201]:

“Where the business information in question can be obtained compulsorily, or is required for some benefit or grant, no claim of prejudice can be made. No prejudice will occur if the information in issue is routine or administrative (that is, generated as a matter of practice).

The agency will usually be best placed to identify, and be concerned about the circumstances where the disclosure of documents might reasonably be expected to prejudice the future supply of information to it.”

The term ‘prejudice’ is not defined in the FOI Act. The FOI Guidelines provide the following definition, at [5.22] – [5.23]:

… The Macquarie Dictionary definition of ‘prejudice’ requires:

a. *disadvantage resulting from some judgement or action of another*
b. *resulting injury or detriment*

A prejudicial effect is one which would cause a bias or change to the expected results leading to detrimental or disadvantageous outcomes. The expected outcome does not need to have an impact that is 'substantial and adverse'.

As outlined above, although reporting eligible data breaches is compulsory, the extent of information provided by an organisation is voluntary. The OAIC recommends the reporting organisation provide additional information relating to the circumstances of the data breach, what the organisation has done to contain the data breach and what, if any, remedial action has been taken to assist the OAIC to investigate the data breach.

Considering the investigation into the CTARS data breach is ongoing, I am satisfied that releasing the information provided by CTARS could reasonably be expected to reduce the quantity or quality of information regarding the data breach provided to the OAIC by reporting organisations in the future.

I am satisfied that a reduction in the quantity or quality of information provided to the OAIC regarding the CTARS data breach could hinder the ability of the OAIC to conduct a full investigation, which may lead to the disadvantageous outcome that an appropriate determination is not made.

Based on the information before me at this time, I am satisfied that disclosure of the documents at this time could reasonably be expected to prejudice the future supply of information to the OAIC for the purposes of reporting Notifiable Data Breaches (s 47G(1)(b)).

Public interest test – s 11A(5)

An agency cannot refuse access to a conditionally exempt document unless giving access would, on balance, be contrary to the public interest (s 11A (5)). In this case, I must consider whether disclosure of the documents would be contrary to the public interest.

Section 11B(3) of the FOI Act lists factors that favour disclosure when applying the public interest test. The FOI Guidelines, at [6.19], include a non-exhaustive list of further factors that favour disclosure.

I consider the public interest factor favouring disclosure in this case is that disclosure would promote the objects of the FOI Act.

I must then balance the factor favouring disclosure against the factors against disclosure. The FOI Act does not specify any factors against disclosure, however the FOI Guidelines, at [6.22], provide a non-exhaustive list of factors against disclosure.

In this case, I consider that the relevant public interest factors against disclosure are:

- disclosure of CTARS' business information could reasonably be expected to have a substantial adverse effect on the investigative functions of the OAIC by discouraging organisations impacted by eligible data breaches from providing the OAIC all information relating to the breach.

- disclosure of CTARS' business information would unreasonably and adversely affect CTARS' commercial activities, through providing an unfair commercial advantage to its competitors and exposing CTARS to the risk of further security breaches.
- disclosure could reasonably be expected to reduce the quantity of information provided to the OAIC by CTARS for the purpose of its ongoing investigation into the data breach.

On balance, in this case, I am satisfied that the public interest factors against disclosure outweigh the public interest factor in favour of disclosure and the relevant documents and material should not be released at this time.

Conclusion

I consider that releasing documents and material in the attached schedule would be against the public interest.

Please see the attached schedule and document.

Please see the following page for information about your review rights and information about the OAIC's disclosure log.

Yours sincerely

Margaret Sui
Senior Lawyer

29 July 2022

If you disagree with my decision

Internal review

You have the right to apply for an internal review of my decision under Part VI of the FOI Act. An internal review will be conducted, to the extent possible, by an officer of the OAIC who was not involved in or consulted in the making of my decision. If you wish to apply for an internal review, you must do so in writing within 30 days. There is no application fee for internal review.

If you wish to apply for an internal review, please mark your application for the attention of the FOI Coordinator and state the grounds on which you consider that my decision should be reviewed.

Applications for internal reviews can be submitted to:

Office of the Australian Information Commissioner

GPO Box 5218

SYDNEY NSW 2001

Alternatively, you can submit your application by email to foi@oaic.gov.au, or by fax on 02 9284 9666.

Further Review

You have the right to seek review of this decision by the Information Commissioner and the Administrative Appeals Tribunal (AAT).

You may apply to the Information Commissioner for a review of my decision (IC review). If you wish to apply for IC review, you must do so in writing within 60 days. Your application must provide an address (which can be an email address or fax number) that we can send notices to, and include a copy of this letter. A request for IC review can be made in relation to my decision, or an internal review decision.

It is the Information Commissioner's view that it will usually not be in the interests of the administration of the FOI Act to conduct an IC review of a decision, or an internal review decision, made by the agency that the Information Commissioner heads: the OAIC. For this reason, if you make an application for IC review of my decision, and the Information Commissioner is satisfied that in the interests of administration of the Act it is desirable that my decision be considered by the AAT, the Information Commissioner may decide not to undertake an IC review.

Section 57A of the FOI Act provides that, before you can apply to the AAT for review of an FOI decision, you must first have applied for IC review.

Applications for IC review can be submitted online at:

https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=ICR_

Alternatively, you can submit your application to:

Office of the Australian Information Commissioner

GPO Box 5218

SYDNEY NSW 2001

Or by email to foidr@oaic.gov.au, or by fax on 02 9284 9666.

Accessing your information

If you would like access to the information that we hold about you, please contact FOIDR@oaic.gov.au. More information is available on the Access our information page on our website.

Disclosure log

Section 11C of the FOI Act requires agencies to publish online documents released to members of the public within 10 days of release, except if they contain personal or business information or information that would be unreasonable to publish.

The document that I have decided to release to you contain material that I have found exempt and would be unreasonable to publish. As a result, an edited version of the document released will be published on our disclosure log.