State Insurance Regulatory Authority

Our reference: BN-06210-2022

Mr Richard Harding
Chief Executive Officer and Managing Director
icare
GPO Box 4052
Sydney NSW 2001

Dear Mr Harding

Letter of Censure – privacy incident relating to the Cost of Claims Report

I refer to the review conducted by the State Insurance Regulatory Authority (**the Authority**) of the recent privacy incident involving the Cost of Claims Report (**Claims Report)** issued by icare on behalf of the Workers Compensation Nominal Insurer (**NI**).

I am writing to advise you that the Authority has finalised its review and is satisfied that the NI has contravened section 243(1) of the *Workplace Injury Management and Workers Compensation Act 1998* (**1998 Act**).

For the reasons outlined below, the Authority has decided to issue the NI with a letter of censure, pursuant to s. 183A of the *Workers Compensation Act 1987* (**1987 Act**).

Section 183A of the 1987 Act provides:
(1) If the Authority is satisfied that a person who is or was a licensed insurer or self-insurer has contravened its licence or this Act or the regulations, the Authority may--
(a) impose a civil penalty on the person not exceeding $50,000, or
(b) issue a letter of censure to the person.

The privacy incident
Pursuant to the workers compensation (**WC**) legislation, the NI is taken to be a licensed insurer. In exercising its licensed insurer functions, the NI receives information relating to WC claims by injured workers, including personal and health information. icare has statutory authority to act on behalf of the NI for the purposes of exercising its insurer functions.

At the relevant time of the incident:
- icare, on behalf of the NI, issued a Claims Report to employers and/or brokers (hereinafter collectively "**employers**") who pay WC premiums to the NI totaling more than $25,000. The Claims Report contained information relating to the WC claims of injured workers, including the personal and health information of those workers.
- The Claims Report was issued to employers as an attachment to an email sent out by a third party provider engaged by icare. No password or other security mechanism was applied to the Report. An email distribution list for the Claims Report was manually prepared by icare and provided to the third party provider.

On 6 May 2022, icare prepared the email distribution list for the Claims Report however data was incorrectly transcribed between spreadsheets resulting in a misalignment of employer email addresses with their policy numbers. The distribution list referred to the third party provider therefore contained incorrect email addresses for some recipients. This meant that when the Claims Report was issued, some employers received personal and/or health information about injured workers whose claims they had no involvement with ("**the privacy incident**").

Approximately 1,450 Claims Reports were emailed to an incorrect address involving approx. 570 incorrect recipients referring to approx. 192,000 injured workers.

icare was notified of the privacy incident by a recipient of an incorrect Claims Report on 10 May 2022. On 13 May 2022, icare verbally advised the Authority about this matter. On 20 May 2022, icare further reported the matter to the Authority.

icare has taken action to remediate the incident and address the processes that contributed to it including:

- contacting recipients of the erroneous emails and seeking confirmation that the Claims Report had been deleted or is inaccessible to them. The Authority understands that in excess of 98% of recipients have provided this confirmation
- providing written notification of the incident to affected workers with open WC claims or claims closed within the last 12 months (subject to some exceptions). The notification included information about mechanisms for complaint and internal review, and counselling for some workers
- engaging third party agencies with relevant expertise to review the incident and provide a harm assessment, and review icare's external reporting processes
- updating the format of the Claims Report to remove personal information and some historical claims information going forward
- implementing post incident controls and processes including additional checks.

Section 243 of the 1998 Act applied to the injured worker information in the Claims Report and made disclosure of that information an offence unless it occurred in one of the exempt circumstances outlined in s. 243(1). The disclosure of the information to the incorrect employers could not have occurred in any of the relevant exempt circumstances.

On 15 August 2022, the Authority issued a show cause notice to icare, on behalf of the NI, outlining the proposed findings of fact as a result of the Authority's review of the matter. By letter dated 5 September 2022, icare accepted the incident was a breach of s243(1) of the 1998 Act, and that it may have been distressing to affected workers. The Authority acknowledges the concession made.

The Authority has considered the entirety of icare's submissions, with all material gathered in the course of its review of the matter, and has determined that:

- in issuing the Claims Report to the incorrect employers on or about 6 May 2022, the Authority is satisfied the NI contravened section 243(1) of the 1998 Act
- a letter of censure is an appropriate outcome for the following reasons:
    - Information relating to thousands of injured workers was sent to incorrect email addresses in the privacy incident with a significant potential risk of distress to those workers
    - There was a lack of appropriate safeguards in place in relation to the handling of the Claims Report notably:
        - Compilation of the distribution list for the Claims Report was reliant on a manual process and therefore at more risk of human error. There is no

evidence of an independent check or verification mechanism in relation to compilation of the list
    - The Claims Report was forwarded to employers by way of email attachment with greater risk of inadvertent disclosure than other means. No encryption, password, or other security mechanism was applied to the Report.

The Authority also notes that it considers the following aspects of icare's response to the incident unsatisfactory:

- Notification to affected workers stated no "personal financial information" was included in the Claims Report. While no banking information was included, the Report did contain information regarding compensation payment amounts which is arguably financial in nature. The Authority considers that the notification should have been clearer on this issue.
- icare originally determined not to notify workers with open psychological claims of the privacy incident due to the potential impact on them. However, the Authority understands icare did send notifications to these workers in error.

This letter of censure will form part of the NI's compliance history. In this instance a letter of censure is considered appropriate, however, in the event the Authority becomes aware of further non-compliance of a similar nature, it may result in an alternative sanction such as the imposition of a civil penalty or prosecution.

In addition, and as specified under section 183A(5) of the 1987 Act, the Authority will publish this letter of censure on Tuesday 4 October 2022.

I remind the NI it must comply with all legislative obligations applicable to licensed insurers. I trust that the Authority's expectations regarding compliance are clear.

Should you wish to discuss this matter, you may contact Christopher White, A/Director, Enforcement & Prosecutions, on [redacted].

Sincerely,

[redacted]

Adam Dent
Chief Executive
State Insurance Regulatory Authority

29 September 2022