AUSTRALIAN COLLECTORS & DEBT BUYERS ASSOCIATION

30 November 2012

Mr Richard Glenn
Assistant Secretary
Business and Information Law Branch
Attorney-General's Department
4 National Circuit
BARTON ACT 2600
By email: privacy.consultation@ag.gov.au

[CONFIDENTIAL]

Dear Richard

SUBMISSION RE AUSTRALIAN PRIVACY BREACH NOTIFICATION

We refer to the Australian Privacy Breach Notification Discussion Paper and in particular the call for submissions.

Australian Collectors & Debt Buyers Association (ACDBA) was established in 2009. Membership is voluntary and open to all debt collectors and debt buyers. Our members[1] represent the majority of the collection market in Australia.

ACDBA and their members support the Privacy Act and the consumer protection measures it affords to the customers of our members.

Our view is that data breach notification should remain voluntary. However, if mandatory privacy breach notification is implemented, we request that the regime find the appropriate balance between the public interest and the compliance burden on industry.

To this end, we make the following submissions (in response to the questions posed in the Discussion Paper) which we hope you give due consideration to:

1.1 Are the current voluntary data breach notification arrangements sufficient?

In our view, the current voluntary data breach notification arrangements find an appropriate balance between consumer protection and industry regulation.

[1] Refer Annexure A for listing of members

Ph: 02 4925 2099
Em: admin@acdba.com
Web: acdba.com

PO Box 295
WARATAH NSW 2298
ABN 18 136 508 784

Furthermore, the Privacy Act and National Privacy Principles (or Australian Privacy Principles) impose sufficiently rigorous standards on organisations to take reasonable steps to protect the unauthorised disclosure or misuse of personal information.

1.2 Should the Government introduce a mandatory data breach notification law?

The Government does not need to introduce a mandatory data breach notification law because the current measures are sufficiently adequate. However, the remainder of this submission will assume comment on the form that a mandatory data breach notification law should, in our view take, if it were to be introduced.

Any regulation surrounding mandatory data breach notification should be principles based rather than prescriptive to afford organisations and agencies some flexibility in responding to a potential data breach bearing in mind the potential risk to affected individuals and the compliance cost to do so.

2.1 What should be the appropriate test to determine the trigger for notification?

The test should be set to an appropriate standard to ensure that immaterial or trivial data breaches do not require notification. Where the data breach involves sensitive information, it may be appropriate for the threshold to be lower than it would be for non-sensitive information. Data breaches on a small or limited scale should also not require notification due to the much lower risk of adverse outcomes for individuals, and the compliance burden that this would place on business.

2.2 Should it be based on a 'catch all' test, or based on more specific triggers, or another test?

We would support a trigger test over a catch all test to give organisations and agencies clarity.

2.3 What specific elements should be included in the notification trigger?

Our first preference for a test would be a trigger test for sensitive information or sensitive personally identifiable information.

Our second preference would be a trigger test of 1,000 breached records.

If a cover-all test were to be used, our preference would be the test suggested by the ALRC of a "real risk of serious harm". Preferably, such a cover-all test would also include some trigger, for example, a number of records, so that isolated instances are not captured under the law.

It would also be necessary to clarify what constitutes 'acquired', 'unauthorised person', 'real risk' and 'serious harm'. It is our view that 'acquired' should be defined so as only to apply when the information is acquired at the initiative of the person who is the acquirer. 'Unauthorised person' should be defined so as to refer only to people to whom it is not contemplated or reasonably foreseeable that such information would be acquired, bearing in mind the purpose for which the information was collected. 'Real risk' should be defined so that it is clear what constitutes 'real'. For example, a one percent risk shouldn't be considered 'real', whereas a fifty percent risk could be considered 'real'. 'Serious harm' should be defined so as to be more than embarrassment or offence but actually physical or financial loss so as to ensure that notification related to immaterial disclosures is not captured.

3.1 Who should be notified about the breach?

In our view, the Commissioner should be notified of a data breach. Discretion about notifying individuals should remain discretionary as, depending on the test that is adopted, there could be instances where a data breach is unlikely to adversely affect individuals and they have been unnecessarily alarmed.

3.2 Which of the below should decide whether to notify?

(i) the organisation or agency;
(ii) the Commissioner; or
(iii) the organisation in consultation with the Commissioner.

The organisation or agency should retain the discretion to notify individuals as they are best placed to understand the scale, context and risk to a consumer associated with a particular potential data breach.

4.1 What should be the form or medium in which data breach notification is provided?

Notification to the Commission should be possible via a secure online portal. Should notification to an individual be required and/or appropriate, it should be made via the same method by which an organisation usually transacts with the individual. For example, an organisation may usually deal with an individual by telephone or email, in which case notification via either of these methods could be appropriate.

4.2 Should there be a set time limit for notification or a test based on notifying as soon as practicable or reasonable?

We would support a test requiring notification as soon as practicable. In the event of a data breach, an organisation will often be working to contain the breach and conduct a risk evaluation. Timing to notify the Commission or an individual should factor this in so that the notification compliance obligation does not detract from containment or risk evaluation.

4.3 What should be the content of the notification?

We would support the notification content set out in the discussion paper for notification to both the Commissioner and an affected individual, that is:

(a) a description of the breach;
(b) a listing of the types of information lost; and
(c) contact details or suggestions for follow up.

5.1 Should there be a penalty or sanction for failing to comply with a legislative requirement to notify?

In our view, the OAIC is an effective regulator with its current enforcement powers and as such, we would see no need for the introduction of a penalty or sanction to be associated with non-compliance with a notification requirement.

Rather than a penalty, discussion or conciliation between the organisation and the Commissioner should be facilitated, with an opportunity for an agreement to be reached about improving processes to avoid a recurrence of the failure to notify.

We also submit that a pecuniary penalty should not be imposed for an inadvertent non-compliance or one where intention and/or recklessness are absent.

5.2 If so, what should be the penalty or sanction, and the appropriate level of that penalty or sanction?

If a penalty or sanction were to be involved, it should a direction to comply or an enforceable undertaking rather than a fine, at least in the first instance.

In our view, any pecuniary penalty should be civil rather than administrative so as to avoid the situation where the commissioner is both investigating and imposing the penalty. Any pecuniary penalty should take into consideration:

(a) the size of the organisation (perhaps by revenue);
(b) the due diligence of the organisation in attempting to prevent a data breach; and
(c) any history of non-compliance with an obligation to notify.

6.1 Who should be subject to a mandatory data breach notification law?

In our view, both agencies and organisations regulated by the Privacy Act should be subject to any mandatory data breach notification law largely the same way.

That notwithstanding, given organisations that are small business operators in accordance with section 6D of the Privacy Act are currently exempt from the National Privacy Principles, we would contend that small business operators under section 6D should also be exempt from any incoming mandatory data breach notification requirement. This would help avoid imposing prohibitive compliance costs on small businesses.

6.2 Should the scope of a mandatory data breach notification law be the same as the existing scope of the Privacy Act?

In our view, the scope of any mandatory data breach notification law should be the same as the existing scope of the Privacy Act.

7.1 Should there be an exception for law enforcement activities?

We make no submissions in respect of this question.

7.2 Would such an exception add anything to the ALRC's proposed public interest exception?

We make no submissions in respect of this question.

We thank you for the opportunity make submissions in respect of this issue. Please contact the writer if you have any questions or wish to clarify any matter raised above.

Yours sincerely
AUSTRALIAN COLLECTORS & DEBT BUYERS ASSOCIATION

Alan Harries
CEO

Ph: 02 4925 2099
Em: akh@acdba.com

Annexure A:

The members of Australian Collectors & Debt Buyers Association are:

- ACM Group Limited
- Austral Mercantile Collections Pty Limited
- Australian Receivables Limited
- Baycorp (Aust) Pty Limited
- Charter Mercantile Pty Limited
- Collection House Limited
- Complete Credit Solutions Pty Limited
- Credit Corp Group Limited
- Credit Four Pty Limited
- Dun & Bradstreet (Australia) Pty Limited
- EC Credit Control Pty Limited
- Insolvency Management Services Pty Limited
- Pioneer Credit Pty Limited
- Shield Mercantile Pty Limited
- State Mercantile Pty Limited
- The ARMS Group Pty Limited