CCCA
ACCJE
Canadian Corporate Counsel Association
Association canadienne des conseillers (ères) juridiques d'entreprises

THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

# Breach of Security Safeguards Regulations under the *Personal Information Protection and Electronic Documents Act*

**CANADIAN BAR ASSOCIATION**
**PRIVACY AND ACCESS LAW SECTION**
**AND CANADIAN CORPORATE COUNSEL ASSOCIATION**

**October 2017**

500–865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
**tel/tél**. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

## PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Canadian Corporate Counsel Association and the Privacy and Access Law Section, both of the CBA, with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law Section and Canadian Corporate Counsel Association.

## TABLE OF CONTENTS

## Breach of Security Safeguards Regulations under PIPEDA

# Breach of Security Safeguards Regulations under PIPEDA

## I. INTRODUCTION

The Canadian Corporate Counsel Association and the Canadian Bar Association Privacy and Access Law Section (the CBA Sections) welcome the opportunity to comment on the draft *Breach of Security Safeguards Regulations* (the Regulations) under the *Personal Information Protection and Electronic Documents Act*[1] (PIPEDA or the Act), as published in *Canada Gazette*, Part I, Vol. 151, No. 35 — September 2, 2017.

The Canadian Bar Association is a national association representing approximately 36,000 jurists across Canada, including lawyers, notaries, academics and law students, and its primary objectives include improvements in the law and the administration of justice. The CBA Privacy and Access Law Section comprises lawyers with an in-depth knowledge of privacy and access to information law, and the Canadian Corporate Counsel Association comprises in-house counsel working for public and private companies, not-for-profit associations, government and regulatory boards, Crown corporations, municipalities, hospitals, post-secondary institutions and school boards

The CBA Sections have made numerous submissions on PIPEDA since its enactment, including our most recent submissions, PIPEDA (March 2017) and PIPEDA Data Breach Notification and Reporting Regulations (May 2016).[2] The CBA Sections recognize that governments and organizations have certain legitimate reasons to collect, use and disclose personal information for limited purposes. We support the principle that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. We also support a balanced approach to the breach notification and reporting regime under PIPEDA,[3] balancing

---

1 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, available online, (http://ow.ly/hcOD30fr4h3).

2 See Canadian Bar Association, *PIPEDA* (March, 2017), available online (http://ow.ly/5pDZ30fr4q8); Canadian Bar Association, *PIPEDA Data Breach Notification and Reporting Regulations* (May, 2016), available online (http://ow.ly/Sf7r30fr4y2).

3 See Division 1.1 of PIPEDA.

individual privacy rights and the legitimate needs of businesses to collect, use and disclose personal information for reasonable purposes. With this perspective in mind, the CBA Sections comment on the Regulations.

## II. REPORT — CONTENT, FORM AND MANNER

The CBA Sections are pleased that the Regulations do not require any identification of types of harm that may result from the breach of security safeguards. The CBA Sections recommended in their June 2014 submission on Bill S-4 – *Digital Privacy Act*[4] that notices and reports not be required to include speculative assessments of the risk of harm. Our expressed concerns with this possible requirement include possible prejudice for the notifying/reporting organization, for example, if an individual claimed damages against the organization based on a privacy breach. The CBA Sections recommended that the content of reports be based on facts:

> The CBA Section encourages an approach to reporting where the contents of a report to the Commissioner are based simply on facts. The BC Information and Privacy Commissioner's Privacy Breach Reporting Form (November 2006) asks for general information about the facts of the breach. The same form also asks the organization to identify types of harm that may result from the breach, which is speculative and may actually discourage proactive reporting. In contrast, a factually based form will encourage reporting. In our view it should be developed by the Commissioner in collaboration with all stakeholders.[5]

Our June 2014 submission also noted that section 19 of Alberta's *Personal Information Protection Act*[6] (PIPA) requires that privacy breach reports to the Privacy Commissioner include "an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure". The CBA Sections are pleased that our recommendation not to include a requirement to identify types of harm from a breach was adopted in the Regulations.

## III. NOTIFICATION TO AFFECTED INDIVIDUAL

### A. Content of Notification

Subsection 10.1(4) of PIPEDA requires notice to be sent to each individual affected by a breach of security safeguards where it is reasonable in the circumstances to believe that the breach

---

4 Canadian Bar Association, *Bill S-4 – Digital Privacy Act* (June, 2014), available online (http://ow.ly/iic330fAmgB).

5 See Canadian Bar Association, *Privacy Act Reform* (June, 2008), cited in Canadian Bar Association, *Bill S-4 – Digital Privacy Act* (June, 2014), available online. (http://ow.ly/h4nr30fAmqO).

6 *Personal Information Protection Act*, SA 2003, c P-6.5, s. 19.

creates a real risk of significant harm to the individual. Section 3 of the Regulations prescribes the content to be included in each notice:

> (f) a toll-free number or email address that the affected individual can use to obtain further information about the breach; and
>
> (g) information about the organization's internal complaint process and about the affected individual's right, under the Act, to file a complaint with the Commissioner.

**Toll-Free Number or Email Address**

The CBA Sections submit that the requirement in section 3(f) of the Regulations to include a toll-free number or email address is too prescriptive and limiting and should be technology-neutral, similar to PIPEDA. Technology-neutral language would provide flexibility in the Regulations and allow organizations to evolve their privacy practices to reflect changing technologies. We expect the Office of the Privacy Commissioner of Canada (OPC) will update its guidance to provide examples of reasonable methods that could be used for obtaining further information, depending on the circumstances, and this may include a physical store or retail location, a toll free number, an email or web site address, social media, text message, or other yet to be developed method of communicating.

**RECOMMENDATION**

1. **The CBA Sections recommend revising section 3(f) of the Regulations as follows:**
   **(f) ~~a toll-free number or email address that~~ a contact method reasonable in the circumstances that the affected individual can use to obtain further information about the breach;**

**Internal Complaint Process**

The requirement in section 3(g) for the notice to include "information about the organization's internal complaint process" is unnecessary and confusing. Section 3(f) already requires the organization to provide contact information for an affected individual to obtain further information about the breach. Section 3(g) also misplaces what should be the emphasis of the communication: that is, giving individuals the necessary information to take steps to protect themselves from harm from a breach of security safeguards, rather than pursuing a complaint with the organization. The emphasis on giving individuals the information to take protective

steps to mitigate or reduce the risk of harm is reflected in Alberta's PIPA and the OPC's guidance, *Key Steps for Organizations in Responding to Privacy Breaches*[7] (the OPC Guidance).

There is no equivalent to section 3(g) of the Regulations in the OPC Guidance or in Alberta privacy regulations. In Alberta, section 19.1(1)(b)(v) of the *Personal Information Protection Act Regulation*[8] (the Alberta Regulation) requires only that the organization provide "contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure" – in other words, an equivalent to section 3(f). Any additional information about an organization's internal complaint process can be obtained through the contact method under section 3(f), similar to the approach in Alberta.

Section 3(g) unnecessarily references "complaint" twice: once in requiring that the content include "the organization's internal complaint process", and again in including information "about the affected individual's right, under the Act, to file a complaint with the Commissioner." This is again in contrast to the OPC Guidance.[9] Imposing an obligation on organizations to expressly encourage affected individuals – twice in section 3(g) – to make a complaint is inappropriate, as the purpose of notification is to provide information to the affected individuals to allow them to mitigate any risk of significant harm related to the breach of security safeguards, rather than on advising them of their right to file a complaint.

In summary, section 3(g) goes beyond current best practice. It should be sufficient for an organization to provide a means by which an affected individual can obtain further information about the breach, which section 3(f) does. Requiring an organization to give further information about its internal complaint process is not the purpose of the notification letter and risks confusing the message it is intended to communicate. Consistent with OPC Guidance, the focus should be on giving the individual a user-friendly message on how they can obtain further information about the breach and what they can and should do to protect themselves.

**RECOMMENDATION**

**2. The CBA Sections recommend deleting section 3(g) of the Regulations.**

---

7 Office of the Privacy Commissioner of Canada, *Key Steps for Organizations in Responding to Privacy Breaches* (August 1, 2007), available online (http://ow.ly/u1Bv30fAmxG) [OPC Guidance].

8 Alta Reg 366/2003, s. 19.1(1)(b)(v).

9 The OPC Guidance does not include information on an organization's internal complaint process. The OPC Guidance suggests including "[t]he contact information for the appropriate privacy commissioner(s)".

## B. Direct Notification — Manner

Section 4 of the Regulations states:

> For the purposes of subsection 10.1(5) of the Act, direct notification is to be given to the affected individual
>
> (a) by email or any other secure form of communication if the affected individual has consented to receiving information from the organization in that manner;
> (b) by letter delivered to the last known home address of the affected individual;
> (c) by telephone; or
> (d) in person.

The CBA Sections have identified a number of concerns, including substantive inconsistencies, with section 4 of the Regulations.

The language in section 4(a) – "any other secure form of communication" – is unclear and awkwardly drafted. On the one hand, letters, telephone calls and in-person notification may also constitute secure forms of communication, but are not referenced. On the other hand, email is not always a secure form of communication, particularly if unencrypted, but the implication is that email is to be considered secure. The CBA Sections propose a simpler categorization: (a) email, (b) secure messaging (if the affected individual has consented to receiving information from the organization in that manner), (c) letter, (d) oral communication by telephone, distinguished from telephone messaging (although it should be clarified whether voicemail would be sufficient), and (e) in-person communications.

Section 4(a)'s consent requirement is also concerning. It is unclear whether the consent requirement is intended to qualify both email and "any other secure form of communication", or just "any other secure form of communication". The use of email insofar as it is being used to alert an individual to a breach of security safeguards should not require that the organization first obtain consent for that use. Neither the OPC Guidance nor the Alberta Regulation have consent requirements. The OPC Guidance advises that direct notification to affected individuals should take place "by phone, letter, email or in person"[10] and the Alberta Regulation requires direct notification generally, but is silent on mechanism. It is unclear then why the Regulations would qualify the use of email by the need for consent. Direct notification is intended to alert individuals to a privacy breach, and to give them an opportunity to reduce the risk of harm resulting from the breach, or to mitigate that harm. Expedited timing is critical to give

---

10 OPC Guidance, available online (http://ow.ly/Boxo30fAmBT).

individuals the best chance at risk mitigation and harm reduction. Imposing a prior consent pre-condition on the ability to send a notification via email reduces the capacity of an organization and individual to achieve that objective.

Moreover, imposing a consent obligation results in unnecessary restrictions on communication where consent was withdrawn or never obtained. For example, if an individual withdrew their consent to use or disclose their personal information one month prior to the breach, is the organization prohibited from using email to contact the affected individual? Or, where the breached personal information was collected and used prior to PIPEDA and archived only for reasonable retention purposes, so no consent was obtained, is the organization prohibited from using an email address in that personal information to contact the affected individual?

A notification email is not a "commercial electronic message", so the consent requirements of Canada's Anti-Spam Legislation[11] would not apply. While the email address may be personal information, requiring consent under section 7(2) of PIPEDA, if PIPEDA permits the use of the email for notification, consent should not be required in the Regulations. In any case, a personal telephone number or home address would also constitute personal information, so it is unclear why only the email address would require consent under the Regulations, and the telephone number and the home address would not.

It is also unclear what "consent" is required to meet the requirement of section 4(a). Given that PIPEDA requires that consent be linked to specific purposes, the Regulations do not specify which of the following consents would be sufficient:

a. "Any" consent: e.g. where the organization obtained consent to use an email to provide a receipt for a purchase;
b. A more general consent "to communicate from time to time information which may be of interest to you"; or
c. A specific consent for privacy breach notification.

Section 4 is also inconsistent in its requirements for addresses and telephone numbers. The mailing address is required to be "home" but the telephone number is not. Care needs to be taken in choosing how communication to affected individuals is made, because these communications could involve sensitive personal information. There is no reason to require

11 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act,* SC 2010, c 23.

that the home address be "the last known" home address, while not requiring that email address and telephone number also be "the last known". Requiring all contact points to be "the last known" is congruent with section 5(1)(c) of the Regulations, where the organization is to give indirect notification to the affected individual where "the organization does not have contact information for the affected individual or the information that it has is out of date."

**RECOMMENDATION**

3. **The CBA Sections recommend revising section 4 of the Regulations as follows:**

   **4 For the purposes of subsection 10.1(5) of the Act, direct notification is to be given to the affected individual using any of the following last known contact information:**

   **(a) by email or any other electronic form of communication used in the normal course to communicate with the affected individual;**
   **(b) by letter delivered to the home address of the affected individual;**
   **(c) by communication to a personal telephone number of the affected individual; or**
   **(d) in person.**

## C. Indirect Notification — Circumstances

Section 5(1) of the Regulations, pursuant to Section 10.1(5) of PIPEDA, permits the organization to give indirect notification to the affected individual in the following circumstances:

> (a) the giving of direct notification would cause further harm to the affected individual;
>
> (b) the cost of giving direct notification is prohibitive for the organization;
>
> (c) the organization does not have contact information for the affected individual or the information that it has is out of date.

The requirement in section 5(1)(c) – the contact information that an organization has is out of date – is too high a threshold to rely on indirect notification. This assists neither the organization seeking to notify nor the individual who ought to receive the notification. The threshold should be a reasonable probability that the contact information is out of date – i.e. that it is likely out of date.

In addition, while the harm test in section 5(1)(a) should be assessed on a per individual basis, the CBA Sections suggest that the tests in Sections 5(1)(b) (prohibitive cost of notification) and 5(1)(c) (not having contact information for the affected individuals) should be assessed against the individuals as a group. The cost of directly notifying the individuals on an individual basis is likely not going to be prohibitive, but the cost of directly notifying all of them as a group may be. Similarly, the organization should be permitted to indirectly notify all the individuals where the organization does not have contact information to directly notify the majority of them.

The CBA Sections propose indirect notification because it is non-specific. For example, in instances where an organization cannot reasonably ensure that it has current personal contact information of an affected individual and the notification itself may contain sensitive personal information, the disclosure of which may harm the individual, indirect, non-specific, notification is appropriate.

**RECOMMENDATION**

4. **The CBA Sections recommend revising sections 5(1)(b) and (c) of the Regulations as follows:**
   **(b) the total cost of giving direct notification to all of the affected individuals is prohibitive for the organization;**
   **(c) the organization generally does not have contact information for the affected individuals or the information it has is likely out of date.**

## D. Indirect Notification — Manner

Section 5(2) of the Regulations, pursuant to section 10.1(5) of PIPEDA, allows indirect notification to be given to the affected individual in the following manner:

> (a) by a conspicuous message, posted on the organization's website for at least 90 days; or
>
> (b) by means of an advertisement that is likely to reach the affected individuals.

For section 5(2)(b), "advertisement" is too narrow a term, and one with inappropriate commercial connotations, and should be replaced with the term "announcement".

**RECOMMENDATION**

5. **The CBA Sections recommend revising section 5(2)(b) of the Regulations as follows:**
   **(b) by means of an announcement that is likely to reach the affected individuals.**

## IV. CONCLUSION

The CBA Sections appreciate the opportunity to offer input on the Regulations. We regularly monitor and recommend improvements to Canada's privacy regime and welcome questions about our submission. We believe that an effective regulatory regime in line with our recommendations will safeguard personal information and strike an appropriate balance between individual privacy rights and the facilitation of commerce.

## V. SUMMARY OF RECOMMENDATIONS

The CBA Sections recommend

1. **revising section 3(f) of the Regulations as follows:**
   **(f) ~~a toll-free number or email address that~~ a contact method reasonable in the circumstances that the affected individual can use to obtain further information about the breach.**
2. **deleting section 3(g) of the Regulations.**
3. **revising section 4 of the Regulations follows:**
   **4 For the purposes of subsection 10.1(5) of the Act, direct notification is to be given to the affected individual using any of the following last known contact information:**
   **(e) by email or any other electronic form of communication used in the normal course to communicate with the affected individual;**
   **(f) by letter delivered to the home address of the affected individual;**
   **(g) by communication to a personal telephone number of the affected individual; or**
   **(h) in person.**
4. **revising section 5(1)(b) and (c) of the Regulations as follows:**

**(b) the total cost of giving direct notification to all of the affected individuals is prohibitive for the organization;**

**(c) the organization generally does not have contact information for the affected individuals or the information it has is likely out of date.**

5. **revising section 5(2)(b) of the Regulations as follows:**

**(b) by means of an announcement that is likely to reach the affected individuals.**