55 University Ave., Suite 603, Toronto, Ontario, M5J 2H7
416.391.2362 ● theCMA.ca

DRAFT GUIDANCE ON BREACH REGULATIONS

Submission to the Office of the Privacy Commissioner of Canada

October 2, 2018

The Canadian Marketing Association (CMA) is the preeminent voice, advocate and advisor of the Canadian marketing profession. The CMA's 400+ members from the private, not-for profit and public sectors share thought leadership, participate in professional development offerings and contribute to a balanced environment where consumers are respected while businesses can thrive. Our Chartered Marketer (CM) designation ensures that marketing professionals are highly qualified and up-to-date with best practices. The CMA champions self-regulatory standards, including a mandatory Code of Ethics and Standards of Practice, plus resources for consumers to better understand their rights.

Office of the Privacy Commissioner of Canada
30 Victoria St., Gatineau, QC
Via email to notification@priv.gc.ca

CMA response to OPC's Draft Guidelines on Mandatory Breach Regulations

The Canadian Marketing Association (CMA) is pleased to respond to the draft guidance document on the mandatory reporting of breaches of security safeguards released by the Office of the Privacy Commissioner of Canada (OPC) on Monday, September 17, 2018. Our members commend the OPC's objective to provide organizations with guidance on how to comply with the breach of security safeguards regulations that go into force on November 1, 2018.

Below we have outlined our position on several elements included in the draft guidance which we believe merit clarification or redrafting.

Reporting. The guidelines indicate that the OPC will expect breach reports from all organizations involved in the breach – including sub-contractors who would not control the personal information processed on behalf of their "controller" clients. In fact, this expectation goes beyond what PIPEDA will legally require once the data breach reporting provisions are in force, as the statutory obligation for reporting falls only to organizations with personal information under their control.

Similarly, the OPC's expectation to deal directly with third party service providers is at odds with the fundamental principle of accountability contained in the Schedule to the Act. As a matter of law, organizations are responsible for personal information under their control, including information that has been transferred to a third party for processing. It is accordingly appropriate that such organizations remain accountable in the event of a breach of security safeguards, including one that might originate with a third-party processor, and be the single reporting entity and point of contact with the OPC in the event of a breach. Moreover, receiving multiple reports from various subcontractors respecting a single breach is only likely to create confusion and increase the administrative burden of reporting, to the detriment of focusing resources on the containment and remediation of the breach, and on efforts to prevent similar breaches in future.

The CMA submits that the guidelines should be revised to remove the expectation of direct reporting by third party processors, but could indicate that the OPC expects that reports from "controller" organizations will be based on relevant input from all parties involved, including subcontractors.

Privilege. With respect to the record-keeping requirement, the guidance indicates that the OPC expects that records of non-reported breaches should include "a brief explanation of why the breach was determined not to pose a "real risk of significant harm." The CMA notes that a determination of whether or not an incident poses a real risk of significant harm, within the meaning of PIPEDA, is a question of law, and will therefore likely be based on a legal opinion, either from inside or outside counsel to the organization in question. Any such opinions would be considered to be protected by

solicitor-client privilege, and the OPC could not compel their production, in line with the Supreme Court of Canada's decision in *Privacy Commissioner of Canada v. Blood Tribe Department of Health*, which held that solicitor-client privilege cannot be set aside by inference but only by legislative language that is clear, explicit and unequivocal. Given that the apparent objective of the record-keeping requirement in the breach notification provisions of PIPEDA is to facilitate oversight of an organization's breach reporting and notification obligations by the Commissioner, who is empowered to require that an organization provide the OPC with copies or access to such breach records on request, the suggestion that privileged advice should be retained for this purpose is problematic. The CMA notes that the guidance already requires a description of the circumstances of the breach and the nature of the information involved. This would allow the OPC, in the case of a review of an organization's breach incident records, to reach preliminary conclusions on compliance with reporting and notification requirements. This could lead to further questions to the organization in question, as necessary, to confirm such an assessment.

The CMA submits that the guidelines should be revised to eliminate the expectation that breach incident records should include an explanation of why the breach was determined not to pose a "real risk of significant harm".

Unnecessary retention of personal information. The guidelines indicate that breach records "need not include" personal details, unless necessary to explain the nature and sensitivity of the information. The CMA notes that, in fact, as required by Principle 5 of the CSA Standard, retention of personal information should be strictly limited to cases where such retention is consistent with the purposes for which it was collected, and where such retention is demonstrably necessary to fulfil those purposes or meet some other legislative obligation. Other sections of the guidelines implicitly recognize this principle and are worded to suggest default behaviour that would comply with Principle 5: for example, when discussing the breach report form, the guidelines indicate that personal information should not be included in a breach report form.

To be consistent with the requirements of PIPEDA, the CMA submits that the guidelines should be revised to indicate that breach records should not include personal details unless necessary to explain the nature and sensitivity of the information.

Form of indirect notification. The Regulations say that indirect notification, where permitted, "must be given by a public communication or similar measure that could reasonably be expected to reach the affected individuals". In its guidance, the OPC goes further than this legal requirement, suggesting that organizations "should employ those measures you would for other public announcements. For example, consider how to incorporate media messaging, including a prominent notice made on your website, or other online/digital presence." These additional measures are not explicitly required by law and may not be required to ensure that the notification could reasonably be expect to reach the affected individuals. They should, at most, only be characterized as factors that an organization may wish to take into account, rather than being presented as measures that an organization "should" take.

The CMA submits that the guidelines should be revised to reflect that the foregoing are suggestions that an organization may wish to take into account, rather than activities that they <u>should</u> undertake.

Breach report form. The proposed form:

- Contemplates a drop-down menu for "type of breach", which contains 4 fixed categories. These options may not apply to all cases. Although presented as an optional field, **the CMA submits that there should be an "other" category to prevent the possibility that organizations may feel compelled to force-fit an incident within one of the fixed categories, and may therefore mis-characterize the breach**.
- Identifies an optional field for "description of relevant security safeguards in place". **The CMA notes that further guidance would be helpful as to the nature of the information that the OPC is contemplating should be included here**, as a list of all relevant security safeguards could be quite detailed, including information on general corporate compliance programs, employee training, contractor selection, etc.
- Seems to contemplate that notification will always be through the proposed breach report form. **The CMA submits that the guidelines should allow for verbal reports, particularly in the period immediately following detection of a breach.** In the midst of breach mitigation and notification of affected individuals, the OPC should not be imposing administrative burden of immediate submission of the reporting form.

Encryption – missed opportunity. The guidelines do raise the concepts of encryption and anonymization/de-identification as factors to be taken into account in determining the probability of misuse, with reference to the statutory test for determining real risk of significant harm. However, the guidelines fall short of noting that robust encryption or reliable, irreversible de-identification would mean very low or no probability of misuse, or even, as other Canadian privacy commissioners have previously ruled, that loss of or access to robustly encrypted data does not constitute a breach, as the information in the hands of any third party could not be used to identify any individual, and would therefore not be considered to be "personal information", within the meaning of PIPEDA. The CMA submits that providing this kind of guidance would not only provide further certainty as to how to assess the extent to which an incident constitutes a breach of security safeguards, and the level of risk that such an incident may create. It would further motivate organizations to implement technical security measures, such as encryption and de-identification, as a means of better securing personal information.

Public disclosure – missed opportunity. The guidelines note that while the OPC is generally required by PIPEDA to keep breach reports confidential, there are a number of exceptions to this requirement, including the possibility of disclosure to the public where the Commissioner considers it to be in the public interest to do so. However, the guidelines provide no signals about cases where public disclosure is unlikely to happen, such as disclosure of details that would have the effect of encouraging similar breaches (for example, widely publicizing a still-open vulnerability, or underlining a potential use or value to hacked PI that might not be widely known/considered). The CMA submits that providing

general assurances as to what would typically not be publicly disclosed, without limiting the OPC's discretion in any particular case, might help encourage greater cooperation and more fulsome reporting by organizations dealing with a breach of security safeguards.

CMA appreciates the opportunity to participate in this important consultation.

For questions or comments regarding this submission, please contact:

Cristina Onosé
Director, Government Relations
conose@theCMA.ca
416-644-3748

*** End of Document ***