# David Young Law
# Compliance Bulletin

**October 2018**

## PIPEDA's Breach Reporting Rules – in force November 1

Effective November 1, 2018 new rules requiring reporting of privacy breaches to the Office of the Privacy Commissioner ("OPC") and notification of affected persons come into force under *the Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The breach reporting provisions were enacted by the *Digital Privacy Act,* passed in 2015 but only now are becoming effective following publication of the enabling regulations.

The new rules mandate reporting, as well as notification, of any "breach of security safeguards" posing a "real risk of significant harm" to individuals. These responses must be made as soon as feasible after discovery of a breach. In addition, the new rules require organizations to keep records of *all* breaches whether or not they meet this threshold.

Enabling regulations, the *Breach of Security Safeguards Regulations,* set out the information that must be included in reports and notifications.

In addition, the OPC has issued guidance[1] to assist organizations in complying with these new requirements, and the nature of records required to be kept under the new rules.

**Threshold requirement for reporting and notification – real risk of significant harm to an individual**

Under the new provisions, both the reporting requirement and the requirement to notify only operate if it is reasonable to conclude that there is a *"real risk of significant harm to an individual"*. To assist making this determination, the PIPEDA provisions provide a non-exhaustive definition of "significant harm"[2] and identify factors relevant to determining whether there is a real risk of such harm to individuals[3].

The OPC's guidance indicates that a *two-tier assessment* is required: first, a determination of the sensitivity of the information compromised by the breach and secondly, a determination of the probability of the information being misused or wrongfully accessed or disclosed. For examples of sensitive information the OPC refers to those cited in the commentary to PIPEDA's Consent Principle - such as medical and financial records. However the guidance also makes clear that the sensitivity of information may be determined by its potential use or misuse. Using this criterion, it may be surmised that even a person's birthdate or home address might be considered sensitive where it could be combined with other information to perpetrate identity theft or financial fraud.

---

[1] *What you need to know about mandatory reporting of breaches of security safeguards* (OPC, Oct.-29, 2018)
[2] S. 10.1(7)
[3] S. 10.1(8)

**David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8**
**T. 416-968-6286 • M. 416-318-5521**
**Privacy and Regulatory Law Counsel • davidyounglaw.ca**

With regard to the second tier of the assessment - probability of misuse, the OPC's guidance provides a list of example questions that may be asked, addressing issues such as: the circumstances of the breach and the likelihood of anyone being harmed; who had access; the length of time the information was exposed; and whether there was any malicious intent. Additional questions point to delving deeper into the known and unknown characteristics of the group of persons to whom the information was made known, so as to assess the likelihood of them misusing the information. Further questions address whether the information was password protected or encrypted or has been recovered.

The OPC's suggested approach to the risk analysis is helpful but may not cast a sufficiently wide net if the goal is to determine whether or not to notify individuals, or report a breach. There are many circumstances which, either in terms of the nature of information exposed or the causes of a breach, may not provide a positive response to the questions listed by the OPC but still could result in a significant risk of harm. An innocent error that leads to the exposure of identity information within a large group not otherwise considered potential misusers may pose a significant risk simply because of the possibility that within that group there may be individuals who might misuse the information.

**Timing and content of reports**

PIPEDA stipulates that a report to the OPC and notification of individuals must be made as soon as feasible after discovery of a breach. The regulations provide direction regarding the form and content of both reports and notifications.

The regulations require that a report to the OPC must be in writing and contain the following information[4]:

(i) the circumstances of the breach and, if known, the cause;
(ii) the day or period, or approximate period, when the breach occurred;
(iii) the personal information subject of the breach, to the extent known;
(iv) the number, or approximate number, of individuals affected;
(v) the steps that the organization has taken or is taking to reduce the risk or mitigate the harm;
(vi) the steps that the organization has taken or is taking to notify affected individuals; and
(vii) contact information of a person at the organization with whom the OPC can communicate.

The OPC has provided an online form for organizations to use in making reports. While the form is not mandatory, it is useful in that it provides prepopulated fields for certain information (e.g. type of breach) and examples of other categories of information (e.g. circumstances of the breach) that will assist respondents in stating the information required to be provided. Using the OPC's form should be the preferred approach if for no other reason than that it should lessen the need for the OPC seeking clarifying information in any follow-up.

[4] While the OPC will receive and develop a file of all reported breaches, there will be no general public disclosure of such breaches. The procedure under the Alberta *Personal Information Protection Act*, which requires the Commissioner to make a determination as to whether notification of a breach is required, can be contrasted with the PIPEDA provision. The Commissioner publishes on her website a report of all breaches for which she has determined notification is required.

**Notification of individuals and other organizations**

Notification of affected individuals must be made as soon as feasible after discovery of a breach and contain sufficient information to allow the individual to understand the significance of the breach and to take steps to reduce the risk of harm. The regulations set out the minimum information that must be included, as follows:

(i) a description of the circumstances of the breach;
(ii) the day or period, or approximate period, when the breach occurred;
(iii) the personal information subject of the breach, to the extent known;
(iv) the steps that the organization has taken to reduce the risk of harm;
(v) the steps that the individual could take to reduce the risk or mitigate the harm; and
(vi) contact information at the organization to obtain further information.

The Act requires that notification be given directly except in circumstances prescribed by the regulations in which case it must be given indirectly. The stipulated circumstances are: if direct notification would cause further harm to the individual; giving direct notification would likely cause undue hardship for the organization (such as a prohibitive cost); or the organization does not have contact information for the individual. The regulations do not specify the means for providing indirect notification but provide a general directive that it must be given by public communication or similar measure that can reasonably be expected to reach the affected individuals. The OPC's guidance gives examples of acceptable media such as newspapers including online versions and prominent notices on corporate websites. The guidance indicates that organizations should use channels that they typically would use for public announcements.

If an organization determines that it must notify individuals, it also must notify any other organization or government institution that may be able to reduce or mitigate the risk of harm resulting from the breach.[5] Such notification must be given within the same time frame as notification to individuals – as soon as feasible after determining that a breach has occurred. These notifications may disclose personal information without consent of the affected individuals.

**Record-keeping requirements**

The regulations, together with the OPC's guidance, provide certain assistance respecting PIPEDA's new requirement for organizations to retain records of all security breaches. Under the regulations, an organization must maintain such records for a minimum of 24 months following the date on which it determined that a breach occurred. The records must contain any information pertaining to a breach that enables the OPC to verify that the organization has complied with the mandatory reporting and notification requirements. The OPC's guidance indicates the minimum information to be maintained, including the date of the breach, a general description of the circumstances including the affected information, and whether or not it was reported to the OPC. The OPC states that the record also should also contain sufficient details for it to assess whether the organization correctly applied the real risk of significant harm standard and otherwise met its obligations to

[5] PIPEDA, s. 10.2(1).

report and notify, including, if the breach was not reported and individuals not notified, a brief explanation of why it was determined that the risk threshold was not met.

The new rules define a "breach of security safeguards" as a loss of, or unauthorized access to or disclosure of, personal information resulting from a breach of the security safeguards mandated by PIPEDA's Security Principle, or a failure to have such safeguards.[6] The PIPEDA principle implies a very broad scope. However the new breach definition does not provide any useful guidance as to what the operative words mean or whether any *de minimus* threshold should be applied.[7] On the other hand, because the scope is limited to incidents which involve an actual loss or unauthorized access, an incident that created only a risk of loss or unauthorized access appears not to fall within the definition and therefore is exempt from the record-keeping requirement.

**Risk minimization strategies**

The new PIPEDA rules establish quasi-criminal offences, punishable by fines, for organizations that knowingly breach the new reporting rules, including the record-keeping requirements. This potential exposure together with the increased public scrutiny, and potential lawsuits, that mandatory reporting will bring make it essential for all organizations to review their breach response protocols and institute adjustments and additional procedures where required.

In addition to establishing criteria and procedures for retaining records, organizations must consider whether they will retain information generated in connection with risk assessments, beyond that required for making the determination of whether a breach meets the reporting threshold. In light of the increased risk of reputational damage – and exposure to lawsuits - resulting from the new mandatory reporting requirements, organizations will need to consider whether, or to what extent, they should protect disclosure of information arising from their internal investigations – such as gap analyses – by means of legal privilege.

Apart from ensuring compliance with the new rules, renewed focus on minimizing privacy and security risks within the organization should be made, with a view to avoiding or reducing the likelihood of breaches occurring, and potentially being reported, in the first place.

*For more information please contact:*
David Young 416-968-6286 david@davidyounglaw.ca


[6] PIPEDA, s. 2(1).
[7] The PIPEDA principle refers to physical, organizational and technical safeguards, appropriate to the sensitivity of the information intended to be protected. By the definition provided, it may be surmised that a breach of another PIPEDA rule not involving "security" such as an intentional or negligent unauthorized use of information does not qualify as a breach under the new rules.