

Helping Your Ideas Take Flight.

PIPEDA Data Breach Notification

Richard Austin

June 2018



Agenda

- I. General Obligation to Notify**
- II. *PIPEDA* Data Breach Notification**
 - A. Scope**
 - B. Reporting Obligation**
 - C. Notice of Breach**
 - D. Record Keeping**
 - E. Whistleblowing**
 - F. Offences**



I. General Obligation to Notify

PIPEDA, Schedule 1

4.1 Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.7 Principle 7 – Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.8 Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information

An illustration on the left side of the slide shows a man and a woman standing on a staircase. The man, on the left, is wearing a blue long-sleeved shirt, black pants, and glasses, with his arms crossed. The woman, on the right, is wearing a green dress and carrying a brown briefcase. They are both looking towards the right. The staircase is composed of green and black steps, and the background is a light green wall with a black horizontal band.

Fraudulent Misrepresentation

- A false representation or statement
- Which was knowingly false
- Which was made with the intention to deceive the data subject
- Which materially induced the data subject to act and
- Which caused the data subject damage

May extend to promissory statements such as the prospective disclosure and use of personal information, e.g. in Privacy Policies stating:

“Donor information is maintained in a secured database, and only authorized personnel have access to this information and only for appropriate company purposes.”



Negligence

- Privacy class action lawsuits assert an implied duty to notify data subjects based on standard of care required by a reasonable data custodian
- Absent case law, Plaintiffs assert the standard of care stems from sources such as orders from the federal and provincial privacy commissioners, industry standards and privacy legislation
- For companies experiencing a breach, risk that a notification requirement will be implied based on:
 - Privacy Policies
 - Claim that a reasonable data custodian in the same circumstances would notify its data subjects of the breach.



II. *PIPEDA* DATA BREACH NOTIFICATION

Effective November 1, 2018, under *PIPEDA*, organizations will be

- required to give notice to the federal privacy commissioner, affected individuals and third parties where a ***breach of security safeguards*** creates a ***real risk of significant harm to individuals***;
- required to maintain records of any breach of security safeguards for a two year period; and
- subject to fines of up to \$100,000 for breach of the organization's notification obligations, failure to maintain records of security breaches or breach of provisions of *PIPEDA* protecting data breach notification whistleblowers

An illustration on the left side of the slide shows a man and a woman standing on a staircase. The man, on the left, is wearing a blue long-sleeved shirt, black pants, and glasses, with his arms crossed. The woman, on the right, is wearing a green dress and holding a brown briefcase. They are both looking towards the right. The staircase is composed of green and black steps, and the background is a light green wall with a black horizontal band.

II.A Scope


- Applies to organizations carrying on commercial activities in Canada, other than organizations that are subject to provincial legislation that has been deemed to be substantially similar to *PIPEDA*, e.g.:
 - organizations other than federal works, undertakings or businesses carrying on business only in Alberta, in British Columbia or in Québec
- Not restricted to just Canadian companies:
 - *A.T. v. Globe24h.com*, 2017 FC 114, confirmed that *PIPEDA* applies to companies operating outside Canada if there exists a “real and substantial link” to Canada

An illustration on the left side of the slide shows a man and a woman standing on a staircase. The man, on the left, is wearing a blue long-sleeved shirt, black pants, and glasses, with his arms crossed. The woman, on the right, is wearing a green dress and carrying a brown briefcase. They are both looking towards the right. The staircase is composed of green and black steps, and the background is a light green wall.

II.B Reporting Obligation


- The notification obligations arise when an organization experiences a “**breach of security safeguards**” and it is reasonable in the circumstances to believe that the breach creates a “**real risk of significant harm**” to an individual
- Organization is required to notify
 - the Commissioner
 - the affected individuals
 - any organization that can mitigate the harm caused by the breach
- Notifications must be given as soon as feasible after the organization determines that the breach has occurred

Reporting Obligation



“BREACH OF SECURITY SAFEGUARDS”	“SIGNIFICANT HARM”	“REAL RISK”
<p>Means:</p> <ul style="list-style-type: none">➤ loss of;➤ unauthorized access to;➤ unauthorized disclosure of; <p>personal information that results from a breach of the security safeguards that an organization is required to establish under <i>PIPEDA</i> or from a failure to establish such safeguards (<i>DPA</i>, s. 2.1(3) (<i>PIPEDA</i>, s. 2(1)))</p>	<p>Includes</p> <ul style="list-style-type: none">➤ bodily harm➤ humiliation➤ damage to reputation or relationships➤ loss of employment, business or professional opportunities➤ financial loss➤ identify theft➤ negative effects on the credit record➤ damage to or loss of property <p>(<i>DPA</i>, s. 10 (<i>PIPEDA</i>, s 10.1(7)))</p>	<p>Factors to be considered include:</p> <ul style="list-style-type: none">➤ the sensitivity of the personal information➤ the probability that the information has been, is being or will be misused➤ any other prescribed factor <p>(<i>DPA</i>, s. 10 (<i>PIPEDA</i>, s 10.1(8)))</p>

II.C Notice of the Breach



To Commissioner	To Affected Individuals
<ul style="list-style-type: none">➤ a description of the circumstances of the breach➤ the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period➤ a description of the personal information that is the subject of the breach to the extent that the information is known➤ a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach➤ the name and contact information of a person who can provide more information to individuals about the breach or answer the Commissioner's questions about the breach	
<ul style="list-style-type: none">➤ number of individuals affected➤ cause of the breach (if known)➤ steps taken to mitigate harm resulting from the breach➤ organization's plans to notify affected individuals	<ul style="list-style-type: none">➤ description of the steps that the individuals can take to reduce the risk of harm or to mitigate the harm

An illustration on the left side of the slide shows a man and a woman standing on a platform. The man, on the left, is wearing a blue long-sleeved shirt, black pants, and glasses, with his arms crossed. The woman, on the right, is wearing a green dress and carrying a brown briefcase. They are standing on a grey platform above a set of green stairs. The background is a light green wall with a dark green horizontal band.

Notice of the Breach

- Organizations can send updates to Commissioner with new information the organization becomes aware of
- Notice to Commissioner in writing by secure means of communication
- Notice to individuals:
 - in person
 - by telephone, mail, email or other direct form of communication
- Organization may notify affected individuals indirectly where:
 - direct notification would be likely to cause further harm to the individual
 - undue hardship to the organization
 - the organization does not have the contact information for the affected individual
- Indirect notice must be given by public communication or similar measure that could be reasonably expected to reach the affected individuals
- Organizations must also notify any other organization or government institution of a breach where the other may be able to reduce the risk of or mitigate harm



II.D Record Keeping

- Organizations required to maintain a record of **every** breach of security safeguards involving personal information
- Records are required to include sufficient information for the Commissioner to verify that the organization is complying with its obligations to notify the Commissioner and affected individuals of breaches that create a real risk of significant harm to individuals
- Records need to be maintained for 24 months after the organization determines that the breach has occurred

An illustration on the left side of the slide shows a man and a woman standing on a staircase. The man, on the left, is wearing a blue long-sleeved shirt, black pants, and glasses, with his arms crossed. The woman, on the right, is wearing a green dress and carrying a brown briefcase. They are both looking towards the right. The staircase is composed of green and black steps, and the background is a light green wall with a black horizontal band.

II.E Whistleblowing

PIPEDA:

- entitles a person to give notice to the Commissioner where the person has reasonable grounds to believe that an organization has contravened or intends to contravene the provisions of *PIPEDA* relating to protection of personal information (s. 27)
- prohibits an organization from dismissing, disciplining or otherwise disadvantaging an employee or contractor of an organization because of person's whistleblowing activities (s.27.1).

Protections extended to data breach notification whistleblowers when data breach notification provisions come into force (*DPA*, ss. 22-23).



II.F Offences

Organization that contravenes

- data breach notification provisions in Section 10.1
- obligation to keep and maintain a record of every breach of security safeguards involving personal information
- prohibition against dismissing, disciplining or otherwise disadvantaging a whistleblower

is guilty of:

- an offence punishable on summary conviction and liable to a fine not exceeding \$10,000
- an indictable offence and liable to a fine not exceeding \$100,000
- (*DPA*, s. 28)



Richard Austin
416-941-8210
raustin@dww.com

Deeth Williams Wall LLP
Lawyers, Patent & Trademark Agents

DWW.com