Breach Notification Assessment Tool

December 2006

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Information and Privacy Commissioner of Ontario

David Loukidelis
Commissioner

Ann Cavoukian, Ph.D.
Commissioner

Breach Notification Assessment Tool

The Information and Privacy Commissioners for British Columbia and Ontario have jointly produced this *Breach Notification Assessment Tool* to assist you in making key decisions after a privacy breach occurs. It should be read along with:

B.C.: *Key Steps in Responding to Privacy Breaches*
http://www.oipc.bc.ca

Ontario: *What to do if a privacy breach occurs: Guidelines for government organizations*,
http://www.ipc.on.ca/images/Resources/up-prbreach.pdf

What to do When Faced With a Privacy Breach: Guidelines for the Health Sector,
http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

Organizations that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs. If the breach occurs at a third party entity that has been contracted to maintain or process personal information, the breach should be reported to the originating entity, which has primary responsibility for notification. This *Notification Assessment Tool* takes organizations through four decision-making steps regarding notification:

Step 1: Notifying Affected Individuals

Step 2: When and How to Notify

Step 3: What to Include in the Notification

Step 4: Others to Contact

Step 1: Notifying Affected Individuals

Use the chart below to help you decide whether you should notify affected individuals. If either of the first two factors listed below applies, notification of the individuals affected must occur. The risk factors that follow are intended to serve as a guide. If none of these applies, no notification may be required. You must use your judgment to evaluate the need for notification of individuals.

	Consideration	Check if Applicable ✓
1	**Legislation requires notification** Are you or your organization covered by legislation that requires notification of the affected individual? If you are uncertain, contact the privacy commissioner (see *contact information* at the end of this publication).	
2	**Contractual obligations** Do you or your organization have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?	
3	**Risk of identity theft** Is there a risk of identity theft or other fraud? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial).	
4	**Risk of physical harm** Does the loss of information place any individual at risk of physical harm, stalking or harassment?	
5	**Risk of hurt, humiliation, damage to reputation** Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as mental health records, medical records or disciplinary records.	
6	**Risk of loss of business or employment opportunities** Could the loss of information result in damage to the reputation to an individual, affecting business or employment opportunities?	

Step 2: When and How to Notify Affected Individuals

When: Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

The chart below sets out factors to consider in deciding how to notify the affected individuals.

Considerations Favouring Direct Notification of Affected Individuals	Check if applicable ✓
The identities of the individuals are known.	
Current contact information for the affected individuals is available.	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach.	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification of Affected Individuals	
A very large number of individuals are affected by the breach such that direct notification could be impractical.	
Direct notification could compound the harm to the individual resulting from the breach.	

Step 3: What to Include in the Notification of Affected Individuals

The information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include the information set out below:

Information Required	Confirm Information Included
Date of the breach.	
Description of the breach. A general description of what happened.	
Description of the information. Describe the information inappropriately accessed, collected, used or disclosed.	
Steps taken so far to control or reduce the harm.	
Future steps planned to prevent further privacy breaches.	
Steps the individual can take. Provide information about how individuals can protect themselves, e.g. how to contact credit reporting agencies (to set up credit watch), information explaining how to change a personal health number or driver's licence number.	
Privacy Commissioner contact information. Include information about how to complain to the privacy commissioner.	
Organization contact information for further assistance. Contact information for someone within your organization who can provide additional information and assistance and answer questions.	

Step 4: Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach. Do not share personal information with these other entities unless required.

Authority or Organization	Purpose of Contacting	Check if applicable ✓
Law Enforcement	If theft or other crime is suspected. (Note: The police may request a temporary delay in notifying individuals, for investigative purposes.)	
Privacy Commissioner's Office	For assistance with developing a procedure for responding to the privacy breach, including notification. To ensure steps taken comply with the organization's obligations under privacy legislation.	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body.	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required.	

Contact Information

For public and private sector bodies in British Columbia:

Office of the Information and Privacy Commissioner for British Columbia

Telephone: 250-387-5629

Email: info@oipc.bc.ca

Website: www.oipc.bc.ca

For public and health care sectors in Ontario:

Information and Privacy Commissioner of Ontario

Telephone: 416-326-3333 or 1-800-387-0073

Email: info@ipc.on.ca

Website: www.ipc.on.ca