Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

INTRODUCTION TO KEY STEPS FOR ORGANIZATIONS IN RESPONDING TO PRIVACY BREACHES

The purpose of this document is to provide guidance to organizations when a privacy breach occurs. A privacy breach is the result of an unauthorized access to or collection, use or disclosure of personal information. In this instance, "unauthorized" means in contravention of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* or similar provincial privacy legislation.

Attached are two documents: Key Steps for Organizations in Responding to Privacy Breaches and a Privacy Breach Checklist that will help organizations complete an analysis of the breach using the key steps.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics (Committee) conducted the first mandated 5-year review of *PIPEDA* at the end of 2006. One of the areas of concern both to the members of the Committee, as well as to many witnesses appearing before the Committee, was the appropriate response to a privacy breach by organizations. High-profile data breaches occurring at the end of 2006 reinforced the serious nature of this issue.

The Privacy Commissioner asked the Committee to recommend a legislative amendment to *PIPEDA* to include a breach notification provision. In its Report the Committee recognized the importance of this issue and recommended a modified approach.[1]

In the meantime, the Office has worked in partnership with various stakeholders to develop voluntary guidelines to respond to privacy breaches. A group of private sector organizations, drawing on the helpful documents that had been written by Alberta, BC and Ontario Information and Privacy Commissioners,[2] produced guidelines for discussion with other stakeholders. The Office consulted with private sector organizations and representative associations, as well as civil society groups, and other Privacy Commissioners' offices with substantially similar private sector privacy legislation. These guidelines are a result of this process and the Office appreciates the time and thought that was given to the discussion. Attached is a list of the stakeholders that participated in this process.

1 Recommendations 23, 24 and 25, Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA), Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, Adopted by the Committee on April 24, 2007; Presented to the House on May 2, 2007)

2 http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf ; http://www.oipc.ab.ca/ims/client/upload/Key%20Steps%20in%20Responding%20to%20a%20Privacy%20Breach%202007.pdf ; http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf