4. Keep your purposes for collecting PII narrow and specific — then strictly limit collection to those purposes;

5. Never retain or use PII for purposes other than those you have already stated — this will erode consumer confidence, trust and goodwill;

6. Have processes in place to allow individuals' rights of access and correction to their PII — and to obtain an account of your organization's uses of their PII; and

7. Consider the services of external privacy and security auditors and certification programs — especially when outsourcing PII to partners, affiliates, and third parties for processing.

Privacy Crisis Management Protocol

Be proactive and have a realistic privacy crisis management protocol in place, in the event that a privacy breach occurs:

- *Contain*: Identify the scope of the potential breach and take immediate steps to contain the damage: retrieve all copies of any personal information that has been disclosed;

- *Notify*: Identify those individuals whose privacy was breached and notify them accordingly;

- *Inform*: Ensure appropriate staff within your organization are immediately notified of the breach;

- *Investigate*: Conduct an internal investigation into the matter, linked to any external investigation that may be ongoing;

- *Improve Practices*: Review existing practices and address the situation on a systemic basis, with a view to improving problem areas.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Ann Cavoukian, Ph.D.
Commissioner

Identity Theft

Business Take Note:

Steps to Protect Customer Personal Information

Information and Privacy Commissioner/Ontario

Organizations that place the burden of dealing with identity theft on their customers run the risk of lost sales and market share through poor reputation, damage to brand image, and the unpredictable costs of litigation. Lead by making information privacy and security strategic business priorities. Here are some basic steps that any organization can take to protect itself and, most importantly, protect its customers:

1. Whenever possible, encrypt, sever or mask personal data — don't leave personal information or personally identifiable information ("PII") in clear view;

2. Adopt techniques to render PII inaccessible and of no value if stolen by unauthorized parties;

3. Take inventory of all PII collection points, uses, assets, and disclosures in your organization — you cannot protect what you don't know exists;

4. Identify risks and analyze vulnerabilities to the PII regularly — and take action to address them!

5. Whenever possible, securely delete or destroy unnecessary PII, regardless of the media (e.g., shred paper files, pulverize old hard drives);

6. Avoid centralizing all personal data in one database — avoid granting full access and use privileges to any one individual;

7. Vet employees with access to personal information — including all temporary, part-time employees and outside contractors;

8. Put in place a strong interlocking system of controls on access to, and use of, all sensitive data held by your organization — minimize all unnecessary data exposure or "leakage;"

9. Consider innovative privacy-enhancing technologies to identify, authenticate and authorize customers, employees, and external agents whenever they seek access to PII;

10. Put in place a reliable system to detect and respond to breaches involving personal information — monitor database transaction and access logs;

11. If involved in sales, do not print the entire credit card number on the sales receipt. "Truncate" the printing of the number by only printing the last four digits.

12. Secure your sensitive data with a comprehensive suite of physical, technological and administrative safeguards — consider "in-depth," multi-level security practices; and

13. Train all staff to recognize privacy threats and to respond appropriately — create a culture of privacy in your organization.

General privacy guidelines based on Fair Information Practices:

1. Put in place a comprehensive privacy program for managing personal information throughout your organization, and for mitigating the risks and threats;

2. Ensure that your privacy policies and procedures are easily available to individuals in a clear, complete and timely manner — be prepared to explain and justify your practices;

3. Wherever possible, obtain and record the informed consent of individuals before collecting and using their PII — build trust early on in the relationship;