Privacy Breach

This guideline is intended to help take the appropriate steps in the event of a privacy breach.

A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation or similar provincial privacy legislation. Some of the most common privacy breaches happen when personal information of customers, clients or employees is stolen, lost or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people).

If a privacy breach occurs there are four key steps to consider when responding to a breach or suspected breach: (1) breach containment and preliminary assessment; (2) evaluation of the risks associated with the breach;(3) notification; and (4) prevention. Be sure to take each situation seriously and move immediately to investigate the potential breach. You should undertake steps 1, 2 and 3 either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Step 1: Breach Containment and Preliminary Assessment

You should take immediate common sense steps to limit the breach.

Immediately contain the breach (e.g., stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).

Advise the compliance officer, Oscar Muir, immediately.

If the breach appears to involve theft or other criminal activity, notify the police.

Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

Step 2: Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

(i) Personal Information Involved

(ii) Cause and Extent of the Breach

(iii) Individuals Affected by the Breach

(iv) Foreseeable Harm from the Breach

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit both the organization and the individuals affected by a breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. The challenge is to determine when notices should be required. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is required.

Notifying Affected Individuals

When to notify: Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

How to notify: The preferred method of notification is direct – by phone, letter, email 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 the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. You should also consider whether the method of notification might increase the risk of harm (e.g., by alerting the person who stole the laptop of the value of the information on the computer).

Who should notify: The person that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate.

What: The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:

Information about the incident and its timing in general terms;

A description of the personal information involved in the breach;

A general account of what the organization has done to control or reduce the harm;

What the organization will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number (SIN), personal health card or driver's licence number.

Others to Contact

Privacy Commissioners:

Police: if theft or other crime is suspected.

Insurers or others: if required by contractual obligations.

Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.

Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm.

Other internal or external parties not already notified:

Organizations should consider the potential impact that the breach and notification to individuals may have on third parties and take actions accordingly. For example, third parties may be affected if individuals cancel their credit cards or if financial institutions issue new cards.

Step 4: Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, we need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention and collection policies, etc.);
- a review of employee training practices; and
- a review of service delivery partners (e.g., dealers, retailers, etc.).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.