What to Do When Your Privacy Is Breached

By Bev Hooper

Unfortunately, some of you may have opened your mail at the end of a busy day only to find a letter advising you that your personal information has been breached. What this is referring to, of course, is the unauthorized use and/or disclosure of your personal information. The impacts of such an occurrence can range from minor inconvenience to full-on identity theft.

Privacy breaches can be caused by a number of factors, including employee error, system error, theft, or an employee intentionally accessing personal information when there is no work-related need to do so. Breaches caused by employee or system error are typically not as concerning as those caused by either external or internal theft or by employees intentionally gaining unauthorized access.

Identity theft is one of the most common criminal offenses in Canada. It refers to the act of acquiring and collecting someone else's personal information for criminal purposes. It occurs when someone else takes possession of your personal information, such as your name, address, social insurance number, personal health number, credit card information, and/or your driver's licence. The criminal's intention is to assume your identity and make purchases with your credit cards—and, in some extreme cases, sell your property and embezzle the money. Statistics show that Canada's largest credit bureaus, Equifax and Trans Union, receive between 1,400 and 1,800 identity theft complaints every month. [1]

So how do you know how much risk you're dealing with?

The answer to that question is that you never really know the level of risk until it's too late. There are, however, some steps you should take to help prevent identity theft from occurring; and if you have already become a victim of identity theft, there are steps you can take to reduce the impacts.

How to prevent identity theft?

The best way to prevent identity theft is to understand how thieves can get their hands on your information. The most common way for a thief to begin the process of assuming your identity is via your mailbox: Thieves will steal your mail, rummage through recycle containers, and even piece together confidential documents that you've shredded. Their goal is to obtain information such as banking statements, credit card bills, health-related correspondence (containing your personal health number), and tax notices. They may even file fake change of address forms in order to redirect your mail. Thieves may also access your information by gaining access to unsecured websites where you've provided personal information, including credit card information. They may also pose as telephone solicitors looking for donations.

It is important to remember that the process of assuming your identity may be achieved over an extended period of time, as thieves typically proceed slowly with the hopes of not alerting the victim.

Some tips to help prevent identity theft:

- Use a secured mailbox where mail may be deposited but not accessed without a key or other securing mechanism.
- Do not share personal information on the Internet without checking to ensure that the website is secure (look for a yellow padlock in the corner of your screen).
- Don't feel compelled to provide your credit card number over the phone when making a charitable donation. All legitimate charities will be able to send you documentation in the mail to support their cause (at which point you can review the information for authenticity).
- Advise your credit card companies and utility companies if you suddenly stop receiving your monthly statements in the mail.
- Use cross-cut shredders instead of strip shredders to dispose of confidential documents.
- Use firewalls on your home computer system and secure wireless networks.
- Don't provide too much personal information when signing up for consumer services or programs. You only need to provide as much information as is reasonably needed for the service that you are signing up for. Example: The shopping club doesn't need your social insurance number for you to shop there!
- Review your bank statements and credit card statements regularly to identify any unauthorized activity.

What to do if you have, or suspect you have, fallen victim to identity theft?

Do not hesitate to call your local police. In addition, contact your financial institutions, including their credit card departments, advise them of the unauthorized activity, and request cancellation of fraudulent transactions. Ensure that all credit cards are cancelled, and have new accounts opened. Advise the various credit bureaus of the situation and request that they place a flag on your account—this flag will ensure that any applications for credit submitted under your name are confirmed with you prior to approval. Finally, it is important that you remain especially diligent in reviewing all activity concerning your finances for several years.

While none of us are truly immune from this activity, and from time to time privacy breaches will occur, there are many ways that we can reduce our risk. And remember, if a breach occurs, you can minimize losses if you act quickly!!

Bev Hooper, is the president of Hooper Access and Privacy Consulting Ltd., a Victoria-based company that specializes in privacy awareness, employee computer-based and classroom training, breach mitigation, and privacy compliance audits and reviews. For more free resources, visit: www.hooperconsulting.ca.

Footnote

1. Fasken Martineau, Privacy and Information Protection Bulletin, March 2005 (www.fasken.com).