Office of the
Information and Privacy
Commissioner of Alberta

Personal Information Protection Act

A Snapshot – Two Years of Mandatory Breach Reporting

(May 2010 to April 2012)

Background:

In May of 2010, the *Personal Information Protection Act* (PIPA) was amended to include a requirement that organizations subject to the Act report a breach of personal information where they determine a real risk of significant harm to an individual exists as a result of the breach. The Office of the Information and Privacy Commissioner (OIPC) reviews all breach reports received from organizations to assess whether notification is required. The Information and Privacy Commissioner has the power to require an organization to notify an individual upon determining that a real risk of significant harm exists to the individual.

From the period of May 1, 2010 until April 30, 2012, the OIPC received 151 breach reports. As of April 30, 2012, of those received:

- 63 breaches resulted in a finding of a real risk of significant harm to an individual requiring notification of the individual(s) affected,
- 51 breaches resulted in a finding of no real risk of significant harm to an individual and no notification was required,
- 24 breaches resulted in a finding that the Commissioner did not have jurisdiction, and
- 13 breaches were still under review.

Millions of people have been affected by these breaches. The number of people impacted per breach ranges from 1 individual to 50 million (420,000 Albertans). The types and sizes of organizations reporting breaches to the OIPC are both large and small and represent various industry sectors. A breakdown of the breach reports received by industry sector is as follows:

- Finance 17%
- Retail 12%
- Insurance 11%
- Professional Services 8%
- Healthcare 7%
- Manufacturing 4%
- Information Services 4%
- Oil and Gas 4%
- Real Estate 3%
- Utilities 2%
- Accommodation 2%
- Construction 1%
- Wholesale 1%
- Administrative Services 1%
- Arts and Entertainment 1%
- Other (personal grooming, business and professional associations, religious organizations, and social services) 21%

Summary of breaches reported to the OIPC:

Four main causes emerge from the 63 breaches in which the Commissioner required notification. They are: human error, theft, compromises to electronic systems and inadequate access controls, as follows:

- 22 breaches caused by human error. There were numerous causes of this type of breach, including inappropriate disposal of personal information, emails sent to the wrong individuals (or viewable to all individuals in a mass email), faxes sent to the wrong person or an unsecure fax, loss of files and portable memory sticks, and disclosure of passwords through social engineering. The highest category of human error is mail and courier, of which there were 10 breaches reported. These breaches were caused as a result of mail delivery to the wrong individual, largely due to mail processing errors and courier packages not reaching the intended recipient.

- 18 breaches caused by theft, primarily due to office and car break-ins. Most of these breaches resulted in the loss of computer devices, including laptops and hard drives; although in a few cases paper documents were also stolen.

- 14 breaches caused by electronic system compromises. Generally, these breaches were found to occur as a result of targeted network attacks by external hackers seeking to extract large amounts of data. It is this type of breach where the largest numbers of individuals were affected by a single breach; 50 million in one instance.

- 9 breaches caused by a failure to adequately control access to electronic or paper files resulting in unauthorized access to or disclosure of personal information. In one case the files were accessible to the general public via the Internet.

Full copies of all notification decisions can be found on the OIPC website at the following link:

http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecisions.aspx.

Of the 51 breaches reported where the Commissioner did not require notification of the affected individuals 37 were caused by human error (email and mail being the main causes of this type of breach), significantly more than the other causes of breaches reported; 6 were caused by theft, 4 by system compromise, and 4 were caused by inadequate access controls.

In the Commissioner's decisions, the reasons for finding a real risk of significant harm requiring notification as opposed to a finding of no real risk of significant harm not requiring notification vary.

An analysis of the decisions resulting in a real risk of significant harm shows that most of the personal information breached was considered to be of high sensitivity (see the table containing the types of personal information breached attached to this Report). For example, Social Insurance Numbers, Drivers' License Numbers, credit card numbers, along with expiry date and in some cases the code on the back (called the CCV code), usually in combination with other personal identifiers such as name and address are considered highly sensitive personal information. Highly sensitive personal information coupled with circumstances where information was stolen for nefarious purposes, or where the recipients could not be determined, or where electronic devices containing the personal information had no encryption and no audit capability making access possible and unknown, led to a finding that a real risk of significant harm exists as a result of the breach.

There were a few decisions involving only the loss of email addresses, considered to be of low sensitivity, where a real risk of significant harm was found to exist. The reason for finding that a real risk of significant harm existed in these cases had to do with the large number of affected individuals, often in the hundreds of thousands or more, and the likelihood that the email addresses would be used for a nefarious purpose, such as phishing[1].

An analysis of the breach decisions where no real risk of significant harm was found to exist shows that most of the personal information breached was of low sensitivity. For example, names, addresses and phone number, membership information including fees, email addresses, low risk financial information such as mortgage balance and RESP balance, and product purchase information. In most of these decisions, the reason for finding that no real risk of significant harm existed was due to a finding that the recipients were few and known to the organization or that the information was returned or confirmed destroyed in a relatively short time frame from the date of loss. There are a few decisions involving a breach of highly sensitive information among these decisions. The reason for finding that no real risk of significant harm existed in these cases was due to the organization's use of strong encryption, making access to the information highly unlikely, and audit capability, giving the organization the ability to confirm the personal information had not been accessed.

[1] Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by appearing as a legitimate business website and extracting personal information from unsuspecting victims.

What can be learned from the breaches reported?

Section 34 of PIPA requires that an organization take reasonable steps to safeguard personal information. The information contained in this Report may assist organizations in recognizing areas of risk and provide an opportunity to prevent these types of risk from occurring. The best ways for an organization to prevent a breach include:

1. Limit the amount of personal information collected only to that which is reasonably needed to meet business requirements.

2. Develop procedures involving the handling of personal information with privacy protection in mind, including breach notification procedures, and develop policies to support the procedures established.

3. Train staff to thoroughly understand the importance of protecting personal information and have staff sign a confidentiality agreement acknowledging their obligation to protect personal information.

4. Ensure proper contract controls are in place binding contractors and third parties to the organization's privacy policies, procedures including training, and include a requirement that the contractor promptly notify the organization in the event of a breach.

5. Keep personal information only as long as is necessary to meet business and legal requirements then securely destroy the information.

The document titled "Causes of Breaches and Breach Prevention Recommendations" attached to this Report provides recommendations designed to assist organizations to reduce the risk of breaches of personal information of the type reported to our Office.

For organizations wishing to assess the quality of their security and access controls around personal information, a Security Self-Assessment Tool has been developed collaboratively by this Office, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Privacy Commissioner of Canada. The tool is designed for use by both small and large organizations.

Conclusion:

Even if an organization has proper security controls in place, a security breach can occur. On the OIPC website is a publication titled The Key Steps to Responding to Privacy Breaches which is designed to assist organizations in understanding what to do when a privacy breach occurs.

Organizations need to be vigilant in protecting against a breach of personal information to reduce the risk of harm to their employees, customers and clients. The cost of a breach to an organization can be significant in terms of dollars and in time and resources spent to contain and manage a breach. The most significant cost to an organization as a result of a breach may be the cost to an organization's reputation. Having a good privacy management program in place within an organization is the best way to reduce the risk that a breach of personal information will occur and maintain its reputation as trustworthy. See Getting Accountability Right with a Privacy Management Program developed by OIPC,

the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Privacy Commissioner of Canada for more information on how to develop such a program.

For more information contact:

Calgary: Office of the Information and Privacy Commissioner
Suite 2460, 801 – 6 Avenue SW
Calgary, Alberta T2P 3W2
Phone: (403) 297- 2728
Fax: (403) 297-2711

Types of Personal Information Breached

The information contained in the table below is based on an analysis by the OIPC of the breach reports received between the period of May 2010 to April 2012.

Cause of Breach	**Types of Personal Information Breached** (varies per breach)
Human Error	• Name, address, phone numbers (home and work), email address, date of birth ("DOB"), Social Insurance Number ("SIN"), citizenship, driver's licence number, criminal record, immigration practices, online password, hotel reservations, product purchases, member fees • Employee information (type of employment, employee number, earnings and deductions, income, education and work history, employment performance, termination, T4A statement, pension including beneficiary) • Financial information (RESP information including name of minors, RRSP account and client number, cheque with banking information and signature, T1, notice of assessment, financial statement, credit card number and expiry date, truncated credit card number, net worth, credit report, mortgage application and mortgage balance information) • Medical information (physician's name, mental disorders, blood donor information, blood type, audiogram results)
Theft	• Name, address, phone number, DOB, SIN, email address, driver's licence number, username and password, hair color information, photos of home, children's school, and insurance policy • Employee information (type of employment, payroll, income, offer letter, salary and benefits, discipline) • Financial information (bank account information, credit card number with expiry date) • Medical information (addictions)
System Compromise	• Name, address, phone number, email address, signature, gender, criminal history, passport information, birth certificate information, membership information and frequent flyer information, login name and password (personal and employee), emergency contact condo owner information • Employee information (salary, deposit information, hours worked and work location) • Financial information (credit card holder name, number, expiry date and code on back, bank account number) • Medical information (disability and health care card)
Inadequate Access Controls	• Name, address, phone number, email address, DOB, SIN, driver's licence number, gender, utility account, mailing list with names and contact information • Employee information (salary, discipline, suspension, terminations and safety violations) • Financial information (banking including account number, credit card number plus expiry date and amount charged) • Medical information (counselling notes)