ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-08

The Dominion of Canada General Insurance Company

August 23, 2013

(Case File #P2208)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On November 27, 2012, The Dominion of Canada General Insurance Company (the Organization) provided notice of an incident involving unauthorized access to personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization is an extra-provincial registered corporation operating in Alberta and qualifies as an "organization" as defined in section 1(1)(i)(i) of PIPA.

[6] The Organization reported that the incident involved information about its employees, and, in some cases, their dependants. One hundred and seventeen (117) of the employees are residents of Alberta. The information was contained in the following documents:

- resumes (name, address, contact information, qualifications and credentials, prior work history),
- reference check forms (name, reference, comments),
- employment offer letters (name, employment terms, contact information, salary),
- hiring records (name, reason employment offered, declined or not made by the Organization),
- payroll registers (name, social insurance number, employee number, date of hire, compensation, benefits, deductions, garnishment if applicable, bank account and transit number),
- total compensation statements (name, address, contact information, emergency contact information, compensation, benefit and pension coverage, family status, beneficiary, dependants - name, date of birth, gender and relationship to employee),
- salary garnishments list (name, amount of garnishment, type of order),
- personal and benefit confirmation statements (name, address, contact information, benefit and pension coverage, family status),
- benefits re-enrollment statements (name, benefit and pension coverage),
- retiree benefit confirmation statements (name, address, contact information, benefit and pension coverage, family status, dependant information – name, date of birth, gender and relationship to retiree),
- performance letters and improvement plans (name, performance rating, comments),
- performance rating schedule (name, rating, comments),
- incident reports and investigations (incident details, complainant and witness names, interviews, findings and results),

- disability claims (name, medical information and other information related to claim),
- termination letters, spreadsheets and reports (name, reason for termination and comments),
- exit interview records (name, date of hire, comments),
- list of employees turning 65 (name, date of birth, comments),
- list of employees working from home (name, address, contact information),
- list of volunteers for an Organization event (name and driver's licence number),
- list of employees employed for 25 years or more (name, address, contact information), and
- miscellaneous reports (name, date of birth, address and contact information, compensation, qualifications and credentials).

[8] This information is "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[9] On December 7, 2012, my Office requested the Organization provide additional information concerning this incident. The additional information was provided between December 17, 2012 and January 10, 2013.

[10] The Organization reported the circumstances of the incident as follows:

- On October 18, 2012, four human resources employees discovered they had access to employee folders on the internal network drive that they previously did not have access to.
- The Organization determined an error occurred during a network migration resulting in all authorized users of the Organization's internal network having access to the folders. There are 1,547 authorized users of the internal network, including employees, consultants, and contractors.
- Access controls for the folders were restored on October 18, 2012.
- The folders contained the personal information of 1,300 employees; one hundred and seventeen (117) of these employees are Alberta residents.
- The 4 human resources employees signed undertakings stating they did not view the contents of the folders. However, the Organization cannot confirm if the folders were accessed by other network users as there was no audit capability in place when the incident occurred. The audit capability was deactivated during the network migration but was restored following the incident.
- The Organization is developing recommendations to enhance access controls, logging, monitoring and reporting for the folders.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[11] In considering whether to require the Organization to notify affected individuals of this incident, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[12] Pursuant to section 37.1 of PIPA, I have the power to require that the Organization "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to those individuals as a result of the incident.

[13] In order for me to require that the Organization notify affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[14] The Organization reported that some of the personal information involved in this incident is highly sensitive. It indicated that information in the payroll registers could be used to cause identity theft; medical, termination, workplace incident and performance information could be used to cause hurt, humiliation, damage to reputation and loss of business or employment opportunities. The Organization was of the view that less sensitive information contained in other documents could not be used to cause significant harm to individuals.

[15] In my view, personal information contained in the following documents is moderately sensitive:

- personal and benefit confirmation statements,
- benefits re-enrollment statements,
- list of employees turning 65,
- list of employees working from home,
- list of employees employed for 25 years or more.

[16] Although moderately sensitive, in my view the personal information found in these documents could not be used to cause significant harm to affected individuals. As there is no risk of significant harm, real or otherwise, the Organization is not required to notify those individuals whose information is contained in these documents of this incident.

[17] Information contained in the following documents is of moderate to high sensitivity:

- resumes,
- reference check forms,

- employment offer letters,
- hiring records,
- payroll registers,
- total compensation statements,
- salary garnishment list,
- retiree benefit confirmation statements,
- performance letters and improvement plans,
- performance rating schedule,
- incident reports and investigations,
- disability claims,
- termination letters, spreadsheets and reports,
- exit interview records,
- list of volunteers for an Organization event,
- miscellaneous reports.

[18] Personal information in these documents could be used to cause harm in the form of identity theft, fraud, hurt, humiliation, damage to reputation, and loss of future employment opportunities. In my view, these are significant harms.

[19] In order for me to require the Organization to notify affected individuals, however, there must also be a "real risk" of significant harm to those individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[20] The Organization reported it was unlikely that significant harm would result from this incident for the following reasons:

- The incident did not occur as a result of theft or an intentional act.
- There was no evidence that anyone accessed the personal information in the folders. No complaints were received. The four employees who reported the incident provided undertakings that they did not open the folders.
- The folders were accessible for a limited period of time: September 3, 2012-October 18, 2012.
- The impact of the incident was contained. Access controls were restored immediately following the incident.
- The personal information was only accessible internally, not to the general public.
- All employees are required to comply with the Organization's policies on confidentiality, or risk discipline or termination of employment.

[21] In deciding whether there is a real risk of significant harm to the affected individuals as a result of this incident, I considered previous breach notification decisions P2011-ND-016, P2010-ND-004 and P2012-ND-10.

[22] In P2011-ND-016, former Commissioner Work found a real risk of significant harm existed as a result of 240 employees having unauthorized access to highly sensitive employee files over a period of 15 months. The personal information involved included names and social insurance numbers. In that incident, the organization was unable to determine how many employees accessed the highly sensitive personal information as there was no system audit capability.

[23] In P2010-ND-004 and P2012-ND-10, an important factor in deciding whether there was a real risk of hurt, humiliation and damage to affected individuals was proximity in the employment context. That is, employees having knowledge of highly sensitive personal information about their coworkers gave rise to a real risk of significant harm to the affected individuals.

[24] Based on the above and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the individuals whose personal information is contained in the documents listed in paragraph 17. The personal information was accessible to over 1,500 individuals for over 30 days. This factor, combined with the fact the Organization did not have the ability to audit access, contributed significantly to my decision.

V. Decision

[25] I require the Organization to notify those individuals whose personal information is contained in the documents listed in paragraph 17, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* and notify me in writing it has done so by September 27, 2013.

[26] In accordance with my authority under section 19.1(2) of PIPA, I further require the Organization to notify each affected individual's dependant(s) indirectly by including in the notification to the respective affected individual that the personal information of the dependant(s) was also involved in the incident and a description of that personal information.

Jill Clayton
Information and Privacy Commissioner