ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-10

LAW SOCIETY OF ALBERTA

December 20, 2012

(Case File #P2078)

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 March 6, 2012, the Law Society of Alberta (the "Organization") reported an incident involving the 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] I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The information at issue in this case qualifies as "personal information" as defined in section 1(1)(k) of PIPA, and includes the following:

- recruitment information (first and last name, salary band, position title, status i.e. new, replacement or temporary),
- resignation information (first and last name, salary band, position title, assessment of whether the resignation was positive, zero or a loss to the Organization, reason for resignation),
- termination information (first and last name, salary band, position title, reason for termination including information about whether the exit strategy involved substantial time, energy, effort and negotiation),
- benefits information (first and last name, type of claim i.e. short and/or long-term disability, parental leave, information about whether processing the disability claim was challenging),
- coaching information (first and last name of individuals who received coaching from the Organization's human resources department), and
- performance review information for one individual detailing key accomplishments and successes, skills development, strengths, weaknesses, training and development needs, performance plans, performance rating, etc.

[7] I note that one of the affected individuals is an incorporated contractor (i.e. the individual performed services for the Organization pursuant to a contract between the Organization and the individual's corporation). Information about this individual appears in a table that identifies the Organization's newly recruited employees, terminations, resignations and retirements, and includes an evaluation of the individual's performance in a personal capacity, despite being a representative of his/her corporation. In my view, and consistent with Order P2012-08 previously issued by my office, this information also qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On March 13, 2012, my Office requested the Organization provide additional information concerning this incident. The additional information was provided by the Organization between March 13 and November 19, 2012.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- An employee with the Organization (the "Employee") inadvertently forwarded an email with an attached document (the "Document") containing the personal information of 104 individuals.
- The email was sent to 28 individuals in the Organization (the "Recipients").
- One of the Recipients brought the error to the Employee's attention the day after the email was sent.
- The Organization reports the following steps were immediately taken once it was notified of the error:
    - The Employee sent an email to the Recipients asking them to delete the email at issue.
    - The Organization's Privacy Officer contacted the Recipients to ensure they had deleted the email from their computer (including from their deleted items).
    - The Recipients were asked if they had opened and read the Document.
    - The Recipients were asked to confirm they had not copied the Document or further disclosed it. They were also asked not to discuss the contents of the Document with anyone in the future.
- Twenty-four of the 28 Recipients confirmed to the Organization that they had not opened the Document and had not copied or further disclosed the Document.
- Four Recipients confirmed that they either read or skimmed the Document.
- The Organization did not notify the affected individuals about the incident.

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

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

[11] Pursuant to section 37.1 of PIPA, I have the power to 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." 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 the affected individuals as a result of the incident.

[12] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected 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.

[13] The Organization indicated that the type of harm that could result from the unauthorized access to the personal information by the Recipients is hurt, humiliation and damage to reputation. The Organization reported that the incident did not pose a significant risk of harm to the affected individuals.

[14] For the reasons that follow, I find that 72 of the 104 affected individuals are not at risk of significant harm as a result of the breach.

- Recruitment and coaching information either alone or in combination reveals only that an individual was recruited and/or received coaching (the Organization reported that "coaching" covers a very broad spectrum of activity including providing assistance and advice on a variety of general employment matters). This is the information at issue for 63 of the affected individuals, and is of low sensitivity.

- Information revealing only that someone resigned their position in order to travel is of low sensitivity. This information is at issue for 1 affected individual.

- Recruitment information combined with termination or resignation information and revealing only that an individual was recruited, resigned to travel or relocate, or completed a contract, is of low sensitivity. This information is at issue for 7 of the affected individuals.

- Information that reveals only that an individual went on parental leave and received coaching is of low sensitivity. This information is at issue for 1 individual.

[15] As there is no risk of significant harm to these 72 individuals, real or otherwise, the Organization is not required to notify them of this incident.

[16] For the reasons that follow, however, I find that for 32 of the 104 affected individuals there is a risk of significant harm from embarrassment, hurt, humiliation, and/or damage to reputation as a result of this incident.

- Benefits information that reveals a claim for disability is highly sensitive information either alone or in combination with other information, such as where there is an indication that processing the claim was challenging. This is the information at issue for 10 of the affected individuals.

- Resignation or termination information combined with other information that indicates a poor performance or where the exit strategy was identified as requiring substantial time, energy, effort and negotiation is highly sensitive information. This is the information at issue for 16 of the affected individuals.

- Resignation and coaching information combined with other information, such as a very personal reason for leaving the organization, is moderately sensitive information. This is the information at issue for 2 of the affected individuals.

- Coaching information together with resignation or termination information combined with information indicating the individual expressed concerns related to his or her supervisor or that his or her exit strategy was challenging is moderately sensitive information. This information is at issue for 3 of the affected individuals.

- The performance review information detailing key accomplishments and successes, skills development, strengths, weaknesses, training and development needs, performance plans, performance rating etc. as well as the individual's views about his/her coworkers, is highly sensitive information. This information is at issue for 1 individual.

[17] In order for me to require the Organization to notify these 32 individuals there must also be a "real risk" of significant harm to these individuals resulting from this 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.

[18] The Organization reported to me that the following factors reduce the risk that significant harm will occur:

- The disclosure was accidental and limited to a small, identifiable group of employees.
- The error was discovered within one day of its occurrence.
- Immediate steps were taken to retrieve the document and ensure it was not accessible or disclosed further.
- The individuals who opened the document are employees of the Organization.
- All employees are bound through their employment relationships to maintain the confidentiality of information learned through their employment.
- The employees who opened the document advised the Privacy Officer that they did not copy, forward or discuss the document with anyone, and that they will not discuss the document with anyone.

[19] In determining whether there is a real risk of significant harm to the 32 individuals, I considered the following:

- The personal information is moderately to highly sensitive.
- The information was skimmed or read by 4 of the Recipients.
- The 32 individuals are current or former coworkers of the 4 Recipients.
- The 32 individuals and the 4 Recipients all work in the same industry in the same city.
- The 4 Recipients are required to hold the personal information in confidence by virtue of their employment relationship.

[20] In 2010-ND-004, Commissioner Work decided there was a real risk that an employee would suffer the significant harm of hurt, humiliation or damage to reputation as a result of unauthorized access by coworkers to highly sensitive information about the employee's potential termination. In that case an email was inadvertently sent by an employee to six employees. Commissioner Work determined that it was enough that one employee read the email for a real risk of significant harm to exist to the employee whose personal information was breached.

[21] In Order P2012-02, Adjudicator Raaflaub addressed whether a complainant suffered hurt, humiliation and damage to reputation when her personal information was inadvertently disclosed to another teacher in another city. In finding the complainant did not suffer a serious breach of privacy that would result in any humiliation or damage to reputation in that case, Adjudicator Raaflaub stated the following:

> The fact that the third party was a stranger to the Complainant, and did not work with her, militates against a finding that the Complainant suffered a serious breach of privacy resulting in any humiliation or damage to reputation. It would have been far more serious, in my view, if a co-worker or acquaintance of the Complainant learned the results of her reassessment. A complete stranger would presumably have no interest whatsoever in the Complainant's educational credentials, salary or reassessment, and would not have any desire or opportunity to disseminate that information, for instance as might occur by way of office or school gossip.

[22] Also, in P2012-ND-023 I decided there was a real risk of significant harm to several members of a credit union when their highly sensitive beneficiary information was inadvertently disclosed to other credit union members. A factor in reaching my decision in that case was that these individuals all lived in close proximity.

[23] In my view, mere knowledge by the 4 Recipients of this moderately to highly sensitive personal information in this case is enough to cause the 32 individuals embarrassment, hurt, humiliation and damage to reputation even without further dissemination. The 4 Recipients either read or skimmed the personal information; their knowledge cannot now be erased or deleted. The 4 Recipients are not strangers to the 32 individuals, but are current or former coworkers who work in the same industry as the 32 individuals in the same city.

[24] Based on the information reported to me by the Organization and the foregoing, I have decided that there is a real risk of significant harm to the 32 individuals as a result of this incident.

V. Decision

[25] I require the Organization to notify the 32 individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation"). I require the Organization to notify me it has done so on or before January 25, 2013.

Jill Clayton
Information and Privacy Commissioner