ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-15

MEGLOBAL CANADA INC.

June 27, 2012

Case File # P2096

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 April 4, 2012, MEGlobal Canada Inc. (the "Organization") provided notice of an incident involving the unauthorized disclosure of 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 a corporation registered in the province of Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information of its employees located in Alberta:

- name,
- address,
- social insurance number (SIN), and
- income and withholdings.

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

III. Background

[8] On April 10, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between March 10 and April 17, 2012.

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

- Pursuant to a services agreement, Dow Chemical Canada ULC ("Dow") provides payroll processing services, including preparation of T4 and T4A tax information forms to the Organization.
- On February 27, 2012, the Organization mailed approximately 224 T4 slips to its employees in Alberta.
- The incident was reported to the Organization in reports made by the Organization's employees when they received unsealed envelopes in the mail.
- When the Organization was notified by the employees of the incident, it contacted all employees who had been mailed T4 slips on February 27, 2012.
- The Organization confirmed that 18 employees (the "Affected Individuals") received their T4 slips in envelopes that were unsealed. A mechanical error with an envelope sealing machine resulted in the envelopes being left unsealed.

- The Organization has implemented the following measures as a result of its investigation into the breach:
    - The envelope sealing machine has been fixed.
    - The sealing machine will be inspected quarterly.
    - Sealed envelopes will be inspected after drying to ensure a dry seal has been made.
    - An enhanced audit process has been put in place.
- The Organization proactively notified the Affected Individuals on March 29, 2012.

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 and 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] In its report, the Organization indicated that the personal information at issue is sensitive and could result in identity theft. The Organization also indicated that the risk that the harm will occur is moderate.

[14] The personal information at issue is of high sensitivity. It includes the name, address, and social insurance number of the Affected Individuals. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. In my view, these are significant harms.

[15] In order for me to require the Organization to notify the Affected Individuals, there must also be a "real risk" of significant harm to the Affected 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.

[16] In deciding whether there exists a "real risk" of significant harm in this case to the affected individuals, I considered the following factors:

- The personal information involved is highly sensitive and could be used to commit identity theft or fraud.
- The T4s could have been accessed at many different points during the mailing process.

[17] In Breach Notification Decision 2011-ND-003, Commissioner Work decided that, despite the Organization's inability to confirm whether personal information in a folder that contained human resource information found on a shared drive was actually accessed, there was a possibility that sensitive personal information was viewed or copied. Given the sensitive data elements and the length of time the information was potentially exposed, Commissioner Work decided there was a real risk of significant harm to the affected individuals and required the organization to notify those individuals under section 37.1 of PIPA.

[18] Based on the information reported to me by the Organization and for the foregoing reasons, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

[19] I require the Organization to notify the Affected Individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[20] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent March 29, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner