ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-008

MAF METAL ALLOY FABRICATION LIMITED

May 4, 2011

(Case File #P1810)

I. Introduction

[1] On March 25, 2011, I received a report from MAF Metal Alloy Fabrication Limited ("MAF Ltd.") of an incident involving the unauthorized access to personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that MAF Ltd. notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] 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.

[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 MAF Ltd. is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

[6] MAF Ltd. informed my Office that the reported incident involved an external payroll provider that MAF Ltd. retains to manage payroll processing. The incident involved the external payroll provider's system being compromised by an external source.

[7] Section 5(1) of PIPA states that an organization is responsible for personal information that is in its custody or under its control. In considering whose responsibility it is to notify, section 5(2) provides that for the purposes of the Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with the Act. The information at issue was under the control of MAF Ltd. as it originally provided the information to the external payroll provider. I find that MAF Ltd. is responsible for the external payroll provider's compliance under the Act. If notification is required under the Act, it would be MAF Ltd.'s responsibility pursuant to section 5(2).

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

III. Background

[9] On March 25, 2011, I received a written report from MAF Ltd. describing an incident involving the unauthorized access to personal information.

[10] On April 4, 2011, my Office contacted MAF Ltd. to request that it provide additional information concerning the incident, in order for me to determine whether to require MAF Ltd. to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and email correspondence between April 4 and April 5, 2011.

[11] The circumstances of the incident reported to me are as follows:

- MAF Ltd. uses an external payroll company to process its payroll.

- The accounting administrator of MAF Ltd. noticed that an unauthorized special pay period had been added to their system in addition to three unknown employees. There was an unsuccessful attempt to move money into the bank accounts of the three unknown employees using the unauthorized pay period.
- MAF Ltd. contacted the external payroll company who confirmed their payroll system had been accessed using the authentication information of the accounting administrator to set up the unauthorized pay period and unknown employees.
- The external payroll company confirmed that their system was compromised by a remote source between 10:46 pm and 11:39 pm EST on March 14, 2011.
- The information contained in the electronic payroll database includes social insurance numbers, pay rate, address, occupation, bank account information, and birthdate of 37 current and former employees.
- Neither MAF Ltd. nor the external payroll company could provide an audit trail of exactly what information was viewed or perhaps copied during the time period of the unauthorized access to the payroll system.

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

[12] Pursuant to section 37.1 of PIPA, I have the power to require MAF Ltd. 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 MAF Ltd. to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[13] In order for me to require that MAF Ltd. notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to individuals found on MAF Ltd. payroll database as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[14] In this case, the personal information at issue is of high sensitivity as it includes name, address, social insurance number and bank account information. This type of information has the potential of being used for identity theft.

[15] Even though there is no evidence to confirm that this information was accessed during the setting up of the unauthorized pay period and employees, the possibility did exist. Once contacted by our office, MAF Ltd. also recognized that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm.

[16] In order for me to require MAF Ltd. to notify its employees, however, there must also be a "real risk" of harm to the employee as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[17] In deciding whether there exists a "real risk" of harm in this case, I considered the external payroll company could not provide an audit trail to confirm whether or not this information was or was not viewed or copied. Access into the payroll database using the information of MAF Ltd. accounting administrator could allow the viewing of this information. I also considered the sensitivity of the information.

[18] Given the information reported by MAF Ltd., I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the fact that the type of information involved could be used to commit identity theft which is a significant harm. There is no audit trail to confirm what information was accessed and given the sensitivity of the information, there remains the possibility information in the payroll system was viewed or copied.

V. Decision

[19] Based on the information reported to me by MAF Ltd., I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require MAF Ltd. to notify individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.*

[20] I understand MAF Ltd. notified current employees affected by the incident by way of individual meetings with them and a letter sent on April 6, 2011. MAF Ltd. indicated in correspondence with my Office that they are attempting to find contact information for affected individuals who are no longer employees of the organization. I require MAF Ltd. to inform my Office of their efforts to notify the former employees on or before May 31, 2011.

Frank Work, Q.C.
Information and Privacy Commissioner