ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-032

SOCIETY OF MANUFACTURING ENGINEERS

September 14, 2011

(Case File #P1964)

I. Introduction

[1] On August 23, 2011, I received a report from the Society of Manufacturing Engineers ("SME" or the "Organization") of an incident involving the loss of, and 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 SME 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 SME 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] In considering whether to require SME to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[7] On August 23, 2011, I received a written report from SME describing an incident involving the loss of and unauthorized access to personal information.

[8] On August 24, 2011, my Office contacted SME to request that it provide additional information concerning the incident in order for me to determine whether to require SME to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a telephone call, via e-mail, and from another written submission to me by the Organization between August 24 and August 30, 2011.

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

- On August 10, 2011 an external hacker gained unauthorized access to SME's computer resources. The incident occurred and was discovered on the same day. The incident was discovered during SME's routine security monitoring of its computer system.
- The total number of individuals affected is 44, 114. This number includes a total of 2558 Canadians, and 285 affected Albertans.
- The personal information accessed of the affected individuals was in electronic form and included the following:
    - Full name;
    - Address;
    - Date of birth;
    - Credit card number;
    - Credit card expiration date; and
    - Credit card security code.
- The information accessed related to stored information from SME member transactions with SME in Michigan such as from members ordering books, videos, or other products; or "renewing membership dues".

- The affected server was housed in SME's locked, access-restricted facility. In terms of technical security safeguards in place at the time of the breach, SME reports that the information breached was stored in an encrypted format and was password protected. SME's computer resources were further protected by a monitored firewall system and other information security measures in accordance with the PCI Security Standards Council Data Security Standards. At the time of the breach, SME was level 4 self-assessed PCI compliant. Nevertheless, the intruder was able to view the personal information because the intruder ran an un-encrypt program.
- It is still unknown who accessed the personal information of those affected.

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

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

[11] In order for me to require that SME notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to SME's members as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[12] In this case, the personal information at issue is of moderate to high sensitivity as it includes member name and address, date of birth, and credit card numbers.

[13] In its assessment of harm resulting from the breach, SME believes there is a low to medium risk that harm could result. The reasons cited for the low to medium risk assessment regarding potential harm is due to several factors regarding SME's attempt at mitigating the risk following discovery of the breach. These factors include the following:

- Immediately upon learning of the breach, SME notified all involved credit card merchant service companies and provided them with the information regarding the affected credit cards. This allowed the credit card companies to monitor the affected cards and issue replacements.
- Many of the stored credit card numbers were expired.
- SME notified the major credit reporting agencies of the incident and identified the affected users so as to prevent any adverse consequences to their credit.
- SME promptly notified the affected individuals by both mail and e-mail so they could take other measure to prevent any harm.
- SME has established a toll-free number to assist affected users.
- Local and Federal law enforcement were notified.
- The affected server was removed from operation, and data was transferred to secure servers.

- Finally, SME is undertaking a forensic investigation using a qualified PCI Forensic Investigator for its point of sale environment.

[14] In order for me to require SME to notify its members, however, there must also be a "real risk" of significant harm to the members 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. Further, there must be a cause and effect relationship between the incident and the possible harm.

[15] In deciding whether there exists a "real risk" of harm in this case, I considered that the personal information at issue is of moderate to high sensitivity and includes full name and address, date of birth, and credit card information of individuals. This is information that could be used to commit identity theft, which in my view is a significant harm. In addition, the information at issue has not been recovered.

[16] In this case I did consider the measures that SME undertook in order to detect the breach, and subsequently notify the affected individuals. I acknowledge that the Organization notified on an expedited basis, but in terms of the risk assessment, I have determined that there is a risk of identity theft; that the personal information was accessed and taken by an external hacker; and that information has not been recovered.

[17] Given the information reported by SME, 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 following factors: the type of information involved could be used to commit identity theft, which in my view is a significant harm, and the information was accessed by an external hacker and has not been recovered.

V. Decision

[18] Based on the information reported to me by SME, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require that SME notify the affected individuals. I acknowledge that SME has already notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation.* As such, I do not require SME to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner