



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|---|---|
| Organization providing notice under section 34.1 of PIPA | Mercer (Canada) Limited (Organization) |
| Decision number (file number) | P2013-ND-47 (File #P2535) |
| Date notice received by OIPC | December 6, 2013 |
| Date Organization last provided information | January 17, 2014 |
| Date of decision | May 20, 2014 |
| Summary of decision | There is a real risk of significant harm to the individuals affected by this incident. The organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA). |
| JURISDICTION | |
| Section 1(1)(i) of PIPA “organization” | <p>The Organization is federally incorporated in Canada.</p> <p>I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.</p> |
| Section 1(1)(k) of PIPA “personal information” | <p>The servers or networks targeted may have contained the following information about the Organization’s employees, contractors and candidates for employment:</p> <ul style="list-style-type: none">• name• social insurance number• address• employment and academic histories <p>The vendor has been unable to confirm to the Organization whether this information was compromised.</p> <p>This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.</p> |

| DESCRIPTION OF INCIDENT | |
|--|--|
| <input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure | |
| Description of incident | The information systems of an organization providing contracted services to the Organization were targeted by a hacker. The personal information at issue was maintained on information systems exposed to the hacker. The intrusion began in June of 2013 and continued until September of 2013. |
| Affected individuals | <ul style="list-style-type: none"> • 27,241 current and former employees and contractors were affected. • 177 of these individuals were Canadian. • 3 Albertans are affected. |
| Steps taken to reduce risk of harm to individuals | Credit protection services for two years have been offered to all potentially affected individuals. |
| Steps taken to notify individuals of the incident | Notification sent by mail to all affected individuals on December 6, 2013. |
| REAL RISK OF SIGNIFICANT HARM ANALYSIS | |
| 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. | <p>The Organization recognized the affected individuals may be at risk for identity theft and fraud.</p> <p>In my view, the personal information involved is highly sensitive. It contains social insurance numbers, identity information such as name and address, plus employment and academic history. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. These are significant harms.</p> |
| Real Risk The likelihood that the significant harm 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. | <p>The Organization reported that, due to the sensitivity of the personal information involved, it considered there to be a real risk of significant harm to the affected individuals.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed by a hacker, indicating possible criminal intent.</p> |

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The personal information involves sensitive identity information, including social insurance numbers. The information was exposed to an unauthorized individual(s) as a result of a hack. These factors contributed significantly to my decision.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by letter on December 6, 2013.

The Organization is therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner