



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|---|---|
| Organization providing notice under section 34.1 of PIPA | Carber Holdings (Organization) |
| File number | P2014-ND 49 (File # P2453) |
| Date notice received by OIPC | September 05, 2013 |
| Date Organization last provided information | September 06, 2013 |
| Date of decision | January 27, 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 34.1(1) of the <i>Personal Information Protection Act</i> (PIPA). |
| JURISDICTION | |
| Section 1(1)(i) of PIPA “organization” | <p>The Organization is incorporated in Alberta as an extra-provincial corporation.</p> <p>I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i) of PIPA.</p> |
| Section 1(1)(k) of PIPA “personal information” | <p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• date of birth,• address,• social insurance number,• phone number,• T4 tax forms. <p>Drug and alcohol test results were also at issue for four of the affected individuals resident in Ontario.</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 checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure | |
| Description of incident | <ul style="list-style-type: none"> • On July 30, 2013, two employees discovered five laptops containing the personal information described above were missing from the Organization’s Houston Texas office. • Upon further investigation, the Organization determined the office had been broken into. • The laptops were password protected but not encrypted. • The Organization reported the incident to the Police. |
| Affected individuals | <ul style="list-style-type: none"> • 294 U.S. and 25 Canadian employees were affected. • 21 of the 25 Canadians are Alberta employees. |
| Steps taken to reduce risk of harm to individuals | <ul style="list-style-type: none"> • One year free, credit monitoring was provided. • Computer systems are being monitored for breaches. • Installation of an interior swipe card system. • Alarms and cameras have been installed. |
| Steps taken to notify individuals of the incident | Notification sent by mail on August 09, 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 due to the nature of the personal information.</p> <p>In my view, the personal information involved is highly sensitive. It includes dates of birth and social insurance numbers, as well as drug and alcohol test results for four individuals. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud, as well as possibly hurt, humiliation and embarrassment. In my view, 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 as the personal information was stolen during a break-in and has not been recovered. Furthermore, the laptops were not encrypted.</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 involved is sensitive and could be used to cause harm, the five laptops were stolen and not recovered. The laptops were not encrypted. These factors contributed significantly to my decision.

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

I understand the Organization notified the affected individuals in a letter dated August 09, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner