Office of the Information and Privacy Commissioner of Alberta

**PERSONAL INFORMATION PROTECTION ACT**
**Breach Notification Decision**

| | |
|---|---|
| **Organization providing notice under section 34.1 of PIPA** | Acosta Canada Corporation (Organization) |
| **Decision number (file number)** | P2016-ND-01 (File #000077) |
| **Date notice received by OIPC** | December 23, 2014 |
| **Date Organization last provided information** | November 19, 2015 |
| **Date of decision** | January 13, 2016 |
| **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 *Personal Information Protection Act* (PIPA). |
| **JURISDICTION** | |
| **Section 1(1)(i) of PIPA "organization"** | The Organization is incorporated in Alberta as an extra-provincial corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved names, plus one or more of the following information elements:<br><br>• date of birth,<br>• address,<br>• Social Insurance Number (SIN),<br>• bank account information,<br>• employee identification number,<br>• phone number, and<br>• email address.<br><br>This information is about current and former employees of the Organization and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta. |

| DESCRIPTION OF INCIDENT | |
|---|---|
| ☒ loss ☐ unauthorized access ☐ unauthorized disclosure | |
| **Description of incident** | • On November 10, 2014, a vehicle belonging to an associate in the Organization's Human Resources Department was burglarized in the United States. Some personal items and a company laptop were stolen.<br>• The associate discovered the theft on November 11, 2014.<br>• The laptop contained personal information of current and former employees.<br>• The laptop was password protected but not encrypted.<br>• Local law enforcement was notified of the theft on November 11, 2014.<br>• The laptop has not been recovered to date. |
| **Affected individuals** | • 5330 Albertans were affected by the incident. |
| **Steps taken to reduce risk of harm to individuals** | • Access to one year of complimentary identity protection and restoration services was provided.<br>• Reported the incident to the local Sheriff's Office.<br>• Remote login capabilities for laptop terminated.<br>• Toll-free confidential call centre organized for affected individuals.<br>• Contact information for private sector privacy Commissioners provided and link to "Identity theft what it is and what you can do about it" (Privacy Commissioner of Canada).<br>• The Organization reviewed its policies and procedures relating to the security and confidentiality of records containing personal information and is developing additional policies, controls, and training, in order to prevent the recurrence of such an incident, such as:<br>o Conducting security awareness training courses for all employees with access to personal information.<br>o Implementing policy requiring employees to agree to notify the Organization immediately of a lost or stolen mobile device, including bring your own devices (BYOD).<br>o Encrypting end user devices that contain or have access to personal information, including Human Resources, Finance, Information Technology, and C-level employees. Encryption to include all BYOD used by these users to access the Organization's systems.<br>o Deploying mobile theft management and remote wiping software to all BYOD that potentially have access to or could contain personal information. |

| | |
|---|---|
| | ○ Requiring and implementing mobile device management software on all mobile devices that contain or have access to PII, including Human Resources, Finance, Information Technology, and C-level employees. |
| **Steps taken to notify individuals of the incident** | Notification sent by mail on December 19, 2014. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>Some damage or detriment or injury that could be caused to 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. | The Organization recognized the information at issue "could potentially be used to commit identity theft and fraud".<br><br>I agree with the Organization. The information includes sensitive identity and financial information, as well as email addresses. This information could be used to cause the harms of identity theft and fraud, as well as phishing. These are significant harms. |
| **Real Risk**<br>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. | The Organization reported it did not appear that the information on the laptop was the target of the theft and "there is no evidence of actual unauthorized access or misuse of the information" at this time.<br><br>In my view, the likelihood of harm resulting from this incident is increased because the laptop was stolen, indicating malicious intent. The laptop was not encrypted and has not been recovered. |
| **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 there is a real risk of significant harm to the affected individuals. The information at issue includes sensitive identity and financial information, as well as email addresses. This information could be used to cause the significant harms of identity theft and fraud, as well as phishing. The likelihood of harm resulting from this incident is increased because the laptop was stolen, indicating malicious intent. The laptop was not encrypted and has not been recovered. | |

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 in a letter dated December 19, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner