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** | Stewart & Stevenson Canada Inc. (Organization) |
| **Decision number (file number)** | P2018-ND-014 (File #005337) |
| **Date notice received by OIPC** | April 3, 2017 |
| **Date Organization last provided information** | December 15, 2017 |
| **Date of decision** | January 12, 2018 |
| **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 an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved all or some of the following information:<br>• name,<br>• policy number,<br>• plan sponsor,<br>• employee's division number,<br>• employee's life class,<br>• employment date,<br>• insured date,<br>• claim location,<br>• occupation,<br>• annual earnings,<br>• date of birth,<br>• social insurance number,<br>• language spoken,<br>• gender,<br>• province of residence,<br>• type of coverage required,<br>• name of beneficiary,<br>• relationship to employee, |

| | |
|---|---|
| | • beneficiary's date of birth, and<br>• signature of employee<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. |
| **DESCRIPTION OF INCIDENT** | |
| ☒ loss ❑ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • In 2009, thirty-eight (38) employees were terminated from the Organization and their employee files placed in an envelope, boxed-up and moved to long term storage in the basement of the Organization's facility.<br>• In the fall of 2015, as part of a routine purge of documents that had exceeded their retention period, confidential documents were sent offsite for third party shredding and non-confidential documents were sent for third party recycling.<br>• On February 13, 2017, the Organization learned from a police service that unauthorized third parties were in possession of life insurance enrollment forms used by the Organization to enroll its employees in the Organization-provided insurance benefit plan.<br>• The Organization learned that credit cards were fraudulently obtained or identities misappropriated for 21 former employees, using the information on the insurance forms.<br>• The Organization investigated and believes that insurance forms that were intended for shredding were inadvertently sent to a recycling facility where they were passed on to the unauthorized third party.<br>• The Organization does not believe the insurance forms were taken from its own facility as there were other "higher value" documents readily available there, and none of these were discovered by the police service. |
| **Affected individuals** | The incident affected 38 residents of Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Promptly launched an internal investigation, which included interviews with former employees.<br>• Visited the third party's recycling and shredding facility.<br>• Evaluating options to prevent a recurrence of this incident including having shredding trucks come the Organization's facilities rather than sending documents off-sire, or doing its own shredding. |

| | |
|---|---|
| **Steps taken to notify individuals of the incident** | I understand the Organization notified 17 affected individuals whose identities were not known to have been compromised, by letter on March 22, 2017.<br><br>The Organization did not provide any additional notification to the 21 former employees whose identities were known to have been compromised. The Organization said these individuals were already contacted by the police service and felt that notifying the individuals might cause unnecessary confusion and concern that a second incident had occurred. The Organization does not know what form of notification these individuals received from the police service. |
| **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 reported the possible harm that might result from this incident include identity theft and fraud. "The (police service) determined that credit cards were fraudulently obtained or identities have otherwise been misappropriated…using the information from the Forms."<br><br>I agree with the Organization. The comprehensive identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud. |
| **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 did not specifically assess the likelihood of harm resulting from this incident.<br><br>In my view, there is a real risk of significant harm to individuals resulting from this incident. The incident is the result of malicious intent (deliberate theft of documents) and the information at issue has been used to fraudulently obtain credit cards and misappropriate identities. |
| **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.<br><br>The comprehensive identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud. The incident is the result of malicious intent (deliberate theft of documents) and the information at issue has been used to fraudulently obtain credit cards and misappropriate identities.<br><br>The Organization is required 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 17 affected individuals whose identities were not known to have been compromised, by letter on March 22, 2017.

The Organization did not provide any additional notification to the 21 former employees whose identities were known to have been compromised. The Organization said these individuals were already contacted by the police service and felt that notifying the individuals might cause unnecessary confusion and concern that a second incident had occurred. The Organization does not know what form of notification these individuals received from the police service.

Section 34.1 of PIPA says that "**An organization having personal information under its control** must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of 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."

Pursuant to section 37.1(1) of PIPA, where an organization is required to provide notice under section 34.1, I "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...".

The onus for notifying affected individuals about this incident rests with the Organization under PIPA, not the police service. Further, it is not clear what affected individuals may have been told about the incident, and whether the information provided to them from the police service met section 19.1 notice requirements as set out in the *Personal Information Protection Regulations*.

I require the Organization to confirm to my Office, within ten (10) days of the date of this decision, that all 38 affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner