



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Safway Services Canada (Organization)
Decision number (file number)	P2018-ND-138 (File #009898)
Date notice received by OIPC	October 2, 2018
Date Organization last provided information	October 24, 2018
Date of decision	October 30, 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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• address,• social insurance number,• banking information,• hire on package, and• payroll queries. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information 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 August 28, 2018, an employee with the Organization noticed that 15 boxes containing payroll files were missing from the centralized storage room.

	<ul style="list-style-type: none"> • The Organization became aware that the boxes were missing because there was an obvious gap where the boxes should have been. The Organization believes the boxes contained employee files for employees whose employment was terminated in 2011 and 2015. • On August 30, 2018, the Organization discovered that 2 boxes containing invoices and project specific information were missing from a senior employee’s office. These boxes do not contain personal information, but the Organization believes their disappearance is connected to the loss of the other boxes. • The Organization reported that no alarms were triggered during the time period in question indicating that anyone who entered the building had a key and security code. • To date, the boxes are still missing.
Affected individuals	The incident affected approximately 225 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Conducted an internal investigation. • Changed the lock to the storage room. Items must now be logged as signed out, and a senior employee has the only key. • Checked all of its building access data for the time period in question. • Reviewed visitor logs and found there was only one visitor during the relevant time but this visitor was accompanied by an authorized Organization employee. • Contacted the shredding and cleaning companies. The shredding company did not shred anything of magnitude during the time, and the cleaning staff does not clean the storage room. • Met with staff. No staff member has admitted to any involvement in the removal of the boxes.
Steps taken to notify individuals of the incident	Affected individuals have not been notified to date.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm 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.</p>	<p>The Organization reported that “(u)authorized users may use sensitive and confidential information resulting in possible identity theft, fraud, or financial harm to employees.”</p> <p>I agree with the Organization that the identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss to employees.</p>

<p>Real Risk</p> <p>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>	<p>The Organization reported that it “...cannot provide an assessment of the risk of harm. The Company does not know who removed the boxes or for what purpose. It is possible that someone was simply attempting to cause embarrassment and harm to the Company’s reputation but it is also possible that someone removed the information in order to cause harm to past employees. Due to the amount of boxes and that no one within the building witnessed them leaving the building, another theory we have is that someone mistakenly shredded the documentation within the boxes but has not come forward to confirm this. As our investigation is still ongoing, this conclusion had not yet been accepted.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the cause of the breach (loss) is unknown. The documents in the boxes are missing and have not been recovered. Further, the information may have been exposed for approximately two months.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>The identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss to employees. The likelihood of harm resulting from this incident is increased because the cause of the breach (loss) is unknown. The documents in the boxes are missing and have not been recovered. Further, the information may have been exposed for approximately two months.</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation) and confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.</p>	

Jill Clayton
Information and Privacy Commissioner