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	Saint-Gobain Corporation (Organization)
Decision number (file number)	P2017-ND-62 (File #005481)
Date notice received by OIPC	April 27, 2017
Date Organization last provided information	April 27, 2017
Date of decision	May 23, 2017
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"	I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved information included on pay stubs, pay histories, and T-4 Forms for Canadian Citizens (and W-4 and W-2 Forms for United States citizens). This information typically includes, name, contact information, identity information (e.g. Social Insurance Numbers), employment and financial information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. One Alberta employee of the Organization is affected.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In March 2017, the Organization discovered that a third party obtained unauthorized access to the MyPay system hosted and serviced by the Organization's third-party service provider. • The system is an electronic platform that provides the Organization's employees with web-based access to employment information and payment records through an on-line portal.

	• The service provider investigated, and determined that a third-party accessed the online portal by manipulating the login features. • The information was exposed between approximately April 2016 and March 2017. • The incident was discovered during the week of March 6, 2017, when the Organization was advised by three of its employees that information stored on the online portal had been altered.
Affected individuals	The Organization reported that one (1) Alberta employee was affected by the incident.
Steps taken to reduce risk of harm to individuals	• Immediately notified the third party service provider. The Organization is working with the service provider who investigated and contained the unauthorized access. Further investigation and communications with the Federal Bureau of Investigation are ongoing. • Implemented enhanced security measures to prevent the reoccurrence of this incident and prevent the manipulation of the online portal login features. • Advised employees to remain vigilant and monitor accounts for suspicious activities. • Notifying all employees whose accounts were compromised, to enable them to take the necessary steps to protect themselves in the event the information is misused. Further arranged for all these employees to receive a one-year credit-monitoring membership.
Steps taken to notify individuals of the incident	The Organization notified the affected Alberta resident on April 28, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization reported that "The type of harm that may occur is financial loss, fraud, identity theft or negative effects on a credit record." I agree with the Organization's assessment. The identity, employment, and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.

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.	The Organization reported that "At this time, we are aware of fraudulent tax filings being made on behalf of two SGC employees in the United States" and "There is risk of significant harm to one employee who is a resident of Alberta." The Organization also reported "We regard the overall likelihood of additional harm to employees resulting as low to moderate considering the multiple steps taken to address and remedy the breach." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion). Despite steps taken to address and remedy the breach, the information was exposed for almost a year and has not been recovered, and the Organization is aware of fraudulent tax filings being made.

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 identity, employment, and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion). Despite steps taken to address and remedy the breach, the information was exposed for almost a year and has not been recovered, and the Organization is aware of fraudulent tax filings being made.

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

I understand the Organization notified the affected individual in writing on April 28, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner