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	SSAB Swedish Steel, Ltd. (Organization)
Decision number (file number)	P2018-ND-077 (File #008488)
Date notice received by OIPC	April 26, 2018
Date Organization last provided information	April 26, 2018
Date of decision	July 16, 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 the 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: • name, • address, • social insurance number, • salary. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported the incident impacted the "personal information of two residents of Alberta." To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On March 28, 2018, an employee of the Organization unintentionally disclosed payroll information of other employees to a former employee who had requested their own tax documents.

	• The incident was the result of human error, whereby the employee attached a document to an email sent to the former employee. • The Organization learned of the incident on April 2, 2018 when a current employee reported it, after having been contacted by the former employee. Later the same day, the Organization was informed of at least one more contact between the former employee and another current employee.
Affected individuals	The incident affected 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately contacted the former employee in order to obtain confirmation that the information had not been used or shared with any third party and the attachment had been destroyed. Confirmation was received on April 9, 2018. • Offered affected individuals credit monitoring services for one year. • Implementing increased training for HR employees who have access to sensitive personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on April 9, 2018.
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 did not specifically identify the types of harm that might result from this incident, but reported "…given that the information contained in the email was sensitive in nature (social insurance numbers, addresses and salaries), [the Organization] has taken the view that the prudent course of action to take, bearing in mind the financial security of its employees, was to notify the affected individuals and provide further information relating to this incident." In my view, the contact and identity information at issue could be used to cause the harms of identity theft, fraud and financial loss. Further, salary information could be used to cause the harms of hurt, humiliation and embarrassment, particularly if shared with individuals who have a personal or professional relationship with the affected individuals. These are all 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 "The incident impacted only a small number of …employees and [the Organization] took immediate steps to ensure the incident was contained. As the incident was isolated and only involved one recipient who confirmed that the email attachment and the information contained therein had not been used or shared, and has been deleted, it is unclear if the risk of harm to the small number of individuals concerned would meet a significant harm threshold." Further, the Organization "… has no reason to believe

	the information in question has or will be used in a fraudulent manner by the former… employee". In my view, there is a real risk of significant harm in this case, despite the fact the incident did not result from malicious intent but rather human error, and the unintended recipient confirmed the information "had not been used or shared, and has been deleted". While I agree there is little likelihood that the unintended recipient (who is known to the Organization) would use the information for fraudulent purposes, the information was in fact used by the unintended recipient to contact the affected individuals, which suggests there may be a personal/professional relationship between the affected individuals and the unintended recipient. This use of the information, and the potential relationship, increase the likelihood of hurt, humiliation and embarrassment resulting from this incident.

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 contact and identity information at issue could be used to cause the harms of identity theft, fraud and financial loss. Further, salary information could be used to cause the harms of hurt, humiliation and embarrassment, particularly if shared with individuals who have a personal or professional relationship with the affected individuals. These are all significant harms.

I acknowledge that the incident did not result from malicious intent but rather human error, and the unintended recipient confirmed the information "had not been used or shared, and has been deleted". However, while I agree there is little likelihood that the unintended recipient (who is known to the Organization) would use the information for fraudulent purposes, the information was in fact used by the unintended recipient to contact the affected individuals, which suggests there may be a personal/professional relationship between the affected individuals and the unintended recipient. This use of the information, and the potential relationship, increase the likelihood of hurt, humiliation and embarrassment resulting from this incident.

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 affected individuals in writing on April 9, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner