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	AVI-SPL Canada, Ltd. (Organization)
Decision number (file number)	P2018-ND-129 (File #009691)
Date notice received by OIPC	September 12, 2018
Date Organization last provided information	September 12, 2018
Date of decision	September 27, 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 operates in Alberta and 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, • home address, • start date, • status (active or terminated), • rehired date, • partial social insurance number, • partial date of birth, • RRSP contributions, • overtime pay, • commission, • sick pay, • salary, • bonus payments, and • partial bank account. 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	• A former employee requested his personal information from the Organization. • The Organization obtained the information from its contracted third-party payroll provider, but did not realize the documents provided included the personal information of other former and current employees. • On May 29, 2018, the Organization emailed the document containing the personal information of other employees to the former employee who had requested his own personal information. • The breach was discovered the same day when the former employee informed the Organization that he had received the personal information of others in error.
Affected individuals	The incident affected 37 individuals.
Steps taken to reduce risk of harm to individuals	• Requested the former employee delete the document received in error. • Provided a letter to the former employee reminding him of his confidentiality obligations. • Implemented a practice that requires payroll to password protect e-documents containing personal information prior to sending documents via email to others. • Completed an internal investigation and confirmed the document was not shared with any employees of the Organization.
Steps taken to notify individuals of the incident	Affected individuals were not notified.
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 Company has no reason to believe that the former employee will attempt to use the information for identity theft or fraudulent purposes. The Company further remarks that the most sensitive data is partially redacted. However, the Company acknowledges the personal information that was disclosed, although a result of human error, is of the type that can cause hurt, humiliation and embarrassment to affected individuals. The Company does not consider the harm to be significant and considers it to be contained, as indicated herein, but out of an abundance of caution reports to the Office of the Information and Privacy Commissioner."

	In my view, the employment information (salary, commission, sick pay, bonuses) could be used to cause the harms of hurt, humiliation and embarrassment. 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 reported that "No harm is anticipated as the document was sent to a former employee, who confirmed that the email attachment and the information contained therein would not be used or shared with anyone. The former employee also stated that he has deleted the email". The Organization also said "There is no evidence or reason to believe that the personal information has been misused. Further, the most sensitive information (SIN numbers and dates of birth) were partially redacted" and "The former employee also has contractual and common law obligations to the Company to maintain the confidentiality of the information." I agree with the Organization that the likelihood of identity theft and fraud in this case is low. The incident did not result from malicious intent but rather human error. The unauthorized recipient reported the error to the Organization and is known to the Organization. The unauthorized recipient confirmed that the email and documents were deleted and will not be used or shared. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships.

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 employment information (salary, commission, sick pay, bonuses) could be used to cause the significant harms of hurt, humiliation and embarrassment. The likelihood of identity theft and fraud in this case is low. The incident did not result from malicious intent but rather human error. The unauthorized recipient reported the error to the Organization and is known to the Organization. The unauthorized recipient confirmed that the email and documents were deleted and will not be used or shared. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships.

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) and is required to **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.**

Jill Clayton
Information and Privacy Commissioner