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	ISN Software Canada Ltd. (Organization)
Decision number (file number)	P2017-ND-51 (File #002385)
Date notice received by OIPC	February 9, 2016
Date Organization last provided information	February 9, 2016
Date of decision	May 15, 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"	The Organization is incorporated in Alberta. It operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • mailing address, • social insurance number, • date of birth, • base salary, • hire date, and • assigned team. 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	• An employee of the Organization received an email which appeared to be from the Organization's CEO. The email requested information about the Organization's employees in Excel format. • The employee responded to the email, attaching a password protected Excel spreadsheet containing the requested personal information. • The Organization discovered the breach on February 2, 2016.
Affected individuals	The incident affected 463 employees of the Organization, 20 of whom are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted external counsel and notified Human Resources. • Launched an internal audit. • Notified affected employees. • Notified the FBI. • Reviewed policies and procedures respecting personal information and email practices. • Issued an advisory to employees reemphasizing standard operating procedures and warning employees about responding to suspicious emails. • Organized training sessions for all offices and employees on emailing best practices. • Offered free credit monitoring to affected individuals. • Designated an individual to answer questions from affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent on February 3, 2016.
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 "This information could be used for identity theft or fraud. Moreover, there could be a risk of humiliation or damage to reputation of the affected employees if the recipient of the Excel Spreadsheet were to misuse the salary information." I agree with the Organization's assessment. The identity and employment information at issue could be used to cause the harms of identity theft and fraud, and may negatively impact affected individuals' credit record. The employment information (salary) could be used to cause humiliation or damage to reputation. 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 "the phishing email suggests that there was malicious intent." However, "the risks to the affected employees have been mitigated by the fact [the Organization] acted quickly upon discovering the incident. [The Organization] discovered the incident the same day it occurred and notified the affected individuals quickly thereafter." Further, "there is no evidence that the personal information has been misused" at this time. In my view, the likelihood of harm is increased because the incident resulted from deliberate action (perpetrator impersonated a senior member of the Organization) indicating malicious intent, and the circumstances suggest the information at issue was the target. The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result 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 identity and employment information at issue could be used to cause the harms of identity theft and fraud, and may negatively impact affected individuals' credit record. The employment information (salary) could be used to cause humiliation or damage to reputation. These are significant harms. The likelihood of harm is increased because the incident resulted from deliberate action (perpetrator impersonated a senior member of the Organization), indicating malicious intent, and the circumstances suggest the information at issue was the target. The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result 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 a letter dated February 3, 2016, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner