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	Nerval Corporation (Organization)
Decision number (file number)	P2019-ND-070 (File #011924)
Date notice received by OIPC	February 1, 2019
Date Organization last provided information	February 1, 2019
Date of decision	June 3, 2019
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 Organization's notice to affected individuals indicated that the incident involved the following information: • name, • social insurance number, • address, • wages and deductions. 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	• On January 31, 2019, the Organization mailed out employee T4 slips. The program then emailed out a second set of emails to all employees, but included a co-worker's T4. • All T4s are secured with a password.

	• The incident was discovered on February 1, 2019 when the Organization received an email from a former employee stating that they had received someone else's T4.
Affected individuals	The incident affected 43 individuals.
Steps taken to reduce risk of harm to individuals	Requested unintended recipients "Please delete the co-workers T4 email and clear it from your junk mail".
Steps taken to notify individuals of the incident	The affected individuals were notified by email sent February 1, 2019.
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 the possible harms that may occur as a result of the breach were "Id theft and fraud". I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment.
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 assessed the likelihood of harm resulting from this breach as "Very low - employees would need to know the password to access information", noting that "passworded information only sent". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because the breach resulted from error and not malicious intent. However, the Organization did not report how successful it was in recovering the email or ensuring it was securely deleted and not forwarded. Although password protected, it does not appear the information was encrypted. The unauthorized disclosure was to the Organization's employees who may have personal/professional relationships with the affected individuals.
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. A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment.	

The likelihood of harm resulting from this incident is decreased because the breach resulted from error and not malicious intent. However, the Organization did not report how successful it was in recovering the email or ensuring it was securely deleted and not forwarded. Although password protected, it does not appear the information was encrypted. The unauthorized disclosure was to the Organization's employees who may have personal/professional relationships with the affected individuals.

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

I understand the Organization notified the affected individuals by email sent February 1, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner