



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	NAL Resources Management Limited (Organization)
Decision number (file number)	P2018-ND-147 (File #010028)
Date notice received by OIPC	October 16, 2018
Date Organization last provided information	October 16, 2018
Date of decision	November 15, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify those affected individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• home address,• in some instances, social insurance number, passport number, date of birth. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The Organization reported the information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• The Organization reported that “A Breach of three Outlook 365 accounts occurred. One of the accounts contained personal information which may have been accessed by unauthorized individuals.”

	<ul style="list-style-type: none"> • The incident occurred between September 11-28, 2018. • The breach was discovered on October 4, 2018 by review of a system log of risky sign-ins on an account which generated further investigation by the Organization’s IT team. Three accounts with abnormal sign-ins were identified.
Affected individuals	The incident affected 14 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Immediate password reset on impacted accounts. • Increase in spam filter implemented October 5. • Plan to implement multi-factor authentication for all users in 2019. • Review and enhance security practice based on recommendation from security consultants. • Offered credit watch services to affected individuals.
Steps taken to notify individuals of the incident	The Organization reported that “A letter indicating the issue and offering [sic] credit watch services was distributed to all individuals potentially impacted” by email sent October 15, 2018. The Organization did not provide a copy of the notification.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm Some damage or detriment or injury that could be caused to the 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.</p>	<p>The Organization reported that “Possible harm may be identity theft; fraud”.</p> <p>I agree with the Organization’s assessment. The identity and contact information at issue could be used to cause the significant harms of identity theft and fraud.</p>
<p>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.</p>	<p>In assessing the likelihood of harm resulting from this breach, the Organization reported “The unauthorized nature of the account compromise suggest criminals may be behind the breach, suggesting real risk”.</p> <p>I agree with the Organization’s assessment. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for over two (2) weeks.</p>
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 as a result of this incident.	

The identity and contact information at issue could be used to cause the significant harms of identity theft and fraud. A reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for over two (2) weeks.

I require the Organization to notify affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand from the Organization that “A letter indicating the issue and offering [sic] credit watch services was distributed to all individuals potentially impacted” by email sent October 15, 2018. However, the Organization did not provide a copy of the notification so I am unable to confirm if it was in accordance with the Regulation.

The Organization is required to provide my office with a copy of the notification within ten (10) days of the date of this decision, in order to confirm that it has notified affected individuals in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner