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	Alberta Mining Corporation Limited (including a number of subsidiaries and the Robert F Ruben trust) (Organization)
Decision number (file number)	P2017-ND-147 (File #005415)
Date notice received by OIPC	April 19, 2017
Date Organization last provided information	October 5, 2017
Date of decision	November 6, 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 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, • banking information, • date of birth, and • payroll and benefit enrollment form (including name and date of birth of spouse and child). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The incident occurred in Alberta and concerns former and current employees of the Organization, as well as shareholders, trustees or trust beneficiaries.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Around April 10, 2017, the Organization set up temporary remote access capability to allow an employee to remotely access his/her computer while the normal VPN equipment was repaired. On April 18, 2017, the employee noticed a strange User ID accessing the computer. • The Organization investigated, closed the breach, and then determined that only the data physically stored on the affected computer was accessible during the course of the breach. • The Organization reported that most of the data potentially accessible was corporate data; however the computer also contained personal information. • The Organization believes that the hacker had potential access to personal information but has no way of ascertaining if any of the information was actually accessed.
Affected individuals	The incident affected 17 individuals, including 11 Alberta residents.
Steps taken to reduce risk of harm to individuals	Shut down the temporary firewall rule the same day the breach was discovered.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 19, 2017 and April 20, 2017.
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 harm that might result from this incident include "potential fraud or identity theft". I agree with the Organization. The identity, financial and employment information at issue could be used to cause the harms of identity theft and fraud. 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 "Data was not encrypted" and "The information was available for access for just over 4 days, during a holiday weekend. No data was physically removed from the system. However, there is no way of determining if data was copied or otherwise recorded." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the Organization cannot confirm that the information was not copied or recorded during the 4 days it was accessible.

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, financial and employment information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the Organization cannot confirm that the information was not copied or recorded during the 4 days it was accessible. 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 an email on April 19, 2017 and April 20, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner