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	PetroChina Canada Ltd. (Organization)
Decision number (file number)	P2021-ND-088 (File #013236)
Date notice received by OIPC	September 12, 2019
Date Organization last provided information	September 12, 2019
Date of decision	March 16, 2021
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual whose personal information was collected in Alberta, 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 Organization reported, "No specific compromised or at risk information identified. All activity conducted on the laptop by the end user during the compromise period (Aug 26 - 28, 2019) and information accessible by this system is at risk." To the extent this information is about identifiable individuals and was collected in Alberta, it is "personal information" as defined in section 1(1)(k) of PIPA and PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• Malware (Emotet) was discovered on an end user laptop. • The Organization reported the breach occurred on August 26, 2019 and was discovered August 28, 2019 when data communications from the end user laptop matching known Emotet control characteristics were detected by a cybersecurity system. This system alerted the Organization's Canada Cybersecurity Specialist to the detection.

Affected individuals	The incident affected one (1)individual in Alberta
Steps taken to reduce risk of harm to individuals	• Advised user to update financial account credentials that may have been accessed from the compromised machine during the identified time period of the compromise and shortly before. • The Organization has cybersecurity controls in place and a roadmap to continue maturing them to reduce incidents of malware compromise and associated consequences upon occurrence.
Steps taken to notify individuals of the incident	The affected individual was notified in person and verbally on August 28, 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 "Most significant risk is financial fraud based on unauthorized financial account access". I accept the Organization's assessment that possible harms that could result from this incident include fraud. This is a significant harm.
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 "If advice to update financial account and other authentication credentials was adhered to by the end user, likelihood of this harm occurring is minimal". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it appears to be the result of malicious action (malware). The Organization reported that "Unauthorized disclosure of data has not been confirmed in this incident", but also said that "Emotet is known for data exfiltration often related to financial institution account credentials as well as other capabilities. Based on these capabilities any data entered on or accessible by the compromised system is considered at risk of unauthorized disclosure."
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 individual. The information potentially at risk could be used to cause the harm of fraud. The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious action (malware). The Organization reported that "Unauthorized disclosure of data has not been confirmed in this incident", but also said that "Emotet is known for data exfiltration often related to	

financial institution account credentials as well as other capabilities. Based on these capabilities any data entered on or accessible by the compromised system is considered at risk of unauthorized disclosure."

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

I understand the Organization notified the affected individual in person/verbally on August 28, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner