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	Brion Energy Corporation (Organization)
Decision number (file number)	P2017-ND-110 (File #005902)
Date notice received by OIPC	June 16, 2017
Date Organization last provided information	June 16, 2017
Date of decision	August 4, 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident resulted in unauthorized access to "…some personal information such as compensation rates, performance reviews, vacation schedules, timesheets, and the personal contact information of some employees." 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	• During the afternoon of March 24, 2017, a phishing email was sent from an executive email account to an executive assistant requesting payment of a fraudulent invoice of $42 950.00 to the perpetrator. The attacker actively managed the attack through engaging the assistant in discussion regarding the payment. • The executive account was compromised to perpetrate the attack. All systems and data accessible by the executive were potentially accessible to the attacker.

	• To date no evidence has been found of any data compromise, and the attacker's motivation may have been limited to a fraudulent invoice payment.
Affected individuals	The incident affected four (4) staff members that report to the owner of the breached account.
Steps taken to reduce risk of harm to individuals	Remedial action has been taken on the breached account with password updates to prevent further compromise.
Steps taken to notify individuals of the incident	The four (4) potentially affected individuals were notified via email memorandum issued on April 25, 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 "There has been no harm or data compromise identified to date. There is potential of reputation damage, embarrassment and dischord [sic] should some personal performance review or compensatory information be disclosed." In my view, the contact and employment information at issue could be used to cause the harms of hurt, humiliation, embarrassment and damage to reputation. To the extent email addresses were involved, these could be used to cause the harm of phishing. These are all 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.	In its report, the Organization reported: "From a personal employee perspective, there is minimal liklihood [sic] of personal harm. While the personal data available to the attacker may foster embarrassment, discomfort and create dischord [sic] if disclosed, there is minimal opportunity for readily monetizing this information from the perpetrators perspective. Based on the attacker's behavior of sending a Phish to trigger a monetary payoff and disclose the attackers presence, it is likely [sic] the attacker is primarily interested in a rapid payoff." Further, "An extortion attempt utilizing potentially compromised data as leverage would be lengthy and risky for the attacker. As the value of potentially compromised data continually diminishes with time and there has been no evidence of personal data compromise to date, it is unlikley [sic] this will occur in the future." And, finally "Personal harm from this incident is unlikley."

	In my view, the likelihood of significant harm in this case is increased because the incident was the result of malicious intent (deliberate intrusion and actively managed phishing attack to effect payment of a fraudulent invoice). The Organization cannot confirm that the sensitive information at issue was not compromised, and possibly downloaded to an external source, given that it was accessible to the perpetrator. The compromised information may well have continuing value over time, particularly for later phishing purposes.

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 contact and employment information at issue could be used to cause the harms of hurt, humiliation, embarrassment and damage to reputation. To the extent email addresses were involved, these could be used to cause the harm of phishing. These are all significant harms. The likelihood of significant harm in this case is increased because the incident was the result of malicious intent (deliberate intrusion and actively managed phishing attack to effect payment of a fraudulent invoice). The Organization cannot confirm that the sensitive information at issue was not compromised, and possibly downloaded to an external source, given that it was accessible to the perpetrator. The compromised information may well have continuing value over time, particularly for later phishing purposes.

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 affected individuals were notified via email memorandum issued on April 25, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner