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	SFC Energy Ltd. (Organization)
Decision number (file number)	P2022-ND-063 (File #023830)
Date notice received by OIPC	October 22, 2021
Date Organization last provided information	May 2, 2022
Date of decision	November 18, 2022
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 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 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:
	
	For "current employees":
	• terms of employment, including:
	  ○ contract information,
	  ○ compensation information,
	• employment date ranges, and
	• "attendance and performance reviews."
	
	For "former employees":
	• name,
	• address,
	• email address,
	• telephone number,
	• Social Insurance Number,
	• financial information, including:
	  ○ bank account number,
	  ○ bank branch number,
	  ○ bank name,
	• employment contract information, including:

	○ hire date, ○ compensation, • tax information, • benefits information, including: ○ marital status, ○ void cheque, ○ emergency contact name, ○ emergency contact phone number, ○ name of beneficiary, and • spousal and / or dependent (children) information: ○ name, ○ gender, ○ date of birth, ○ disability status. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 24, 2021, the Organization discovered they were victim to a ransomware attack when employees found a message on their workstations "indicating that their computer had been hacked". • An investigation determined the threat actor gained access to the Organization's network through a vulnerability in Microsoft Exchange. It is believed the threat actor had access to the Organization's systems for approximately two months. • "There are no available logs to identify the threat actor's specific activity within the … network." As such, the Organization did not rule out the possibility that data was exfiltrated by the threat actor.
Affected individuals	The incident affected 104 individuals.
Steps taken to reduce risk of harm to individuals	• Offered former and current employees a credit monitoring and identity theft protection package. • Enhanced certain technical safeguards. • Exploring the addition of other IT security features. • Arranging for annual penetration testing by a third party. • Reviewing document retention protocol. • Upgraded employee training to include testing against common attacks.

Steps taken to notify individuals of the incident	Current and former employees affected by the incident were notified by mail or email on October 13, 2021. Emergency contacts, dependents, and beneficiaries were not notified directly; instead, the Organization said: *These individuals were not provided with direct notification as [the Organization] does not have contact information for these individuals. It is our submission that indirect notice was provided by way of the notice provided to former employees.*
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 did not provide an assessment of possible harm(s). In my view, a reasonable person would consider that current employees' employment information could be used to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships. Former employees' contact, identity, financial, employment and benefits information could be used for identity theft, fraud, or affect credit ratings. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Beneficiary, spouse, or dependent information, especially with respect to children or other vulnerable groups, in combination with former employee location or contact information, could be used to cause the harms of embarrassment, hurt or humiliation. All of the above 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: *There is no risk of significant harm to current employees given the limited and non-sensitive nature of the information that was compromised;* *There is no apparent risk of significant harm to former employees given the results of its dark web search showing no evidence of the compromised data on the dark web;* *In any event, any possible harm to current or former employees has been mitigated through the offer of complimentary 2-year subscription to the TransUnion credit monitoring and identity theft protection package and through the guidance provided in the notice on steps the individuals could take to protect themselves.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the

	personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, possible exfiltration of personal information). A lack of evidence that personal information was misused, or disclosed on the dark web, does not mitigate against future harm as identity theft, fraud, and phishing can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately two months.

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.

Current employees' employment information could be used to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships. Former employees' contact, identity, financial, employment and benefits information could be used for identity theft, fraud, or affect credit ratings. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Beneficiary, spouse, or dependent information, especially with respect to children or other vulnerable groups, in combination with former employee location or contact information, could be used to cause the harms of embarrassment, hurt or humiliation. All of the above are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, possible exfiltration of personal information). A lack of evidence that personal information was misused, or disclosed on the dark web, does not mitigate against future harm as identity theft, fraud, and phishing can occur months or years after a breach. Further, the threat actor had access to the Organization's network for approximately two months.

I require the Organization to notify the 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 the Organization notified affected current and former employees by email on October 13, 2021, in accordance with the Regulation. The Organization is not required to notify those affected individuals again.

I also understand that beneficiaries, spouses, or dependents whose personal information were affected were not notified directly of the incident.

Section 19.1(1)(a) of the Regulation states that notifications required under section 37.1 of the Act must "be given directly to the individual"; however, section 19.1(2) says "… notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization submitted that it "[does] not have contact information for these individuals" and instead, "indirect notice was provided by way of the notice provided to former employees." I accept that indirect notice as described by the Organization is reasonable in this case.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance