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	Soroc Technology Inc. (Organization)
Decision number (file number)	P2021-ND-330 (File #022838)
Date notice received by OIPC	August 9, 2021
Date Organization last provided information	August 9, 2021
Date of decision	March 9, 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: • name, • physical address, • email address, • telephone number, • date of birth, • social insurance number, • employment-related dates (hire date, probation, etc.), • payroll information, • banking information, and • photocopy of identification document such as passport or driver's license. 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 May 7, 2021, the Organization was the subject of a ransomware attack. The incident was discovered when a ransom note was received on the same day. • An investigation determined that the unauthorized third party may have exfiltrated data. • The Organization did not indicate how its environment was breached by the attacker.
Affected individuals	The incident affected 1,942 individuals, including 64 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a cyber forensics firm to investigate. • "Immediately made tactical changes such as password changes". • Revising policies related to directories and firewalls. • Reviewing environment to determine what additional security changes should be implemented. • Provided potentially affected individuals with identity theft and credit monitoring services. • Reported the incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 10, 2021.
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 "that there is a risk of identity theft, fraud and phishing attempts." I agree with the Organization's assessment. A reasonable person would consider the identity (date of birth, social insurance number, passport, driver's license), financial (banking), and employment (dates, payroll, etc.) information at issue could be used to cause the harms of identity theft, fraud, and possibly financial loss. Email addresses could be used for the purpose of phishing or spear-phishing, increasing affected individuals' vulnerability to 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 assessed "that the likelihood that harm could result is moderate." The Organization's notice to affected individuals reads, in part: *We were made aware that the unauthorized third party may have gained access to and copied data which may include the personal information of certain … employees, contractors, former employees and former contractors.* *…* *It is important to note that there is no evidence confirming that all the personal information listed above was compromised or misused.* I accept the Organization's assessment. 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 an unauthorized third party (deployment of ransomware, ransom demand). The Organization did not report how long the records may have been exposed, nor if the records were published online by the attacker. A lack of reported misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a breach.

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.

A reasonable person would consider the identity (date of birth, social insurance number, passport, driver's license), financial (banking), and employment (dates, payroll, etc) information at issue could be used to cause the harms of identity theft, fraud, and possibly financial loss. Email addresses could be used for the purpose of phishing or spear-phishing, increasing affected individuals' vulnerability to identity theft and fraud. These 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 an unauthorized third party (deployment of ransomware, ransom demand). The Organization did not report how long the records may have been exposed, nor if the records were published online by the attacker. A lack of reported misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a breach.

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 individuals by letter on August 10, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner