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	Parkland Corporation (Organization)
Decision number (file number)	P2021-ND-154 (File #020248)
Date notice received by OIPC	March 23, 2021
Date Organization last provided information	May 13, 2021
Date of decision	June 8, 2021
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 operates in Alberta 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, • passport information, • social insurance number, • health card number, • date of birth, • copy of drivers' license, and • employee information such as compensation and bonus information, reasons for absences, and performance reviews. 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	• On August 14, 2020, an employee received a phishing email and clicked on an infected link. • As a result, attackers were able to encrypt files on multiple systems and download data from multiple devices. • On November 14, 2020, a ransomware message appeared on the logon screen of multiple systems. • Throughout the month of December 2020, the attackers uploaded the stolen data, approximately 1.3 TB worth, to a website on the Dark Web.
Affected individuals	The Organization estimates approximately 700 individuals were affected, including 50-100 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained experts to conduct a forensic investigation to determine what happened. • Offered 12 months of credit monitoring to individuals for whom there is a real risk of significant harm. • Reported incident to the Calgary Police Services. • Taking technical steps to further secure the network. • Working with an information security company to conduct a security roadmap in order to identify and implement additional controls and tools. • Providing refresher training to staff on identifying and avoiding phishing attacks.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally, beginning on December 20, 2020. On May 6, 2021, the Organization's legal counsel confirmed that it had "completed all notifications that they consider required."
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: *Some of the information may be usable to conduct identity theft, to conduct fraudulent banking activities, and for future phishing attempts. Other information may be of potential embarrassment for certain individuals.* The Organization also said: *Much of the information is old. For example, of the few passports that were breached, all but one was expired.* I agree with the Organization's assessment. A reasonable person would consider the identity information at issue (date of birth, social insurance number, drivers' licence, passport) could be used to cause the significant harms of identity theft and fraud, even if

	outdated/expired. Employment information could be used to cause the significant harms of hurt, humiliation and embarrassment.
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: *Likelihood of harm is considered low, but because it was taken by criminal actors and posted to a public site on the dark web, there is a potential for harm.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email and ransomware) and the information was exposed on the dark web for more than three 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.

A reasonable person would consider the identity information at issue (date of birth, social insurance number, drivers' licence, passport) could be used to cause the significant harms of identity theft and fraud, even if outdated/expired. Employment information could be used to cause the significant harms of hurt, humiliation and embarrassment.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email and ransomware) and the information was exposed on the dark web for more than three 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 has notified affected individuals verbally, a process that began on December 20, 2020 and was confirmed as completed on May 6, 2021.

Jill Clayton
Information and Privacy Commissioner