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	Dillon Consulting Ltd. (Organization)
Decision number (file number)	P2021-ND-238 (File #018749)
Date notice received by OIPC	December 15, 2020
Date Organization last provided information	December 15, 2020
Date of decision	November 23, 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 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 some or all of the following information: • name, • address, • email address, • telephone number, • social insurance number, • date of birth, • drivers license number, • health card number, • banking and tax information, and • business contact information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization reported that some business contact information of the affected individuals in Alberta might have been affected by the breach. .

	"Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization was a victim of a ransomware attack that encrypted its entire operational IT infrastructure. • On the morning of July 10, 2020, the attackers gained access to four (4) workstations and between July 10 and July 19, 2020, the threat actor was able to compromise multiple servers, encrypting all information, and effectively holding the Organization's operational data hostage. • The ransom note indicted that data was exfiltrated, though it did not describe the data. The attack also resulted in the unauthorized access and downloading of certain information. • The Organization was able to rebuild its systems and restore operations. • The Organization communicated with the threat actor, eventually receiving a log of exfiltrated data and purported confirmation that all data was destroyed. • By early October 2020, an outside IT forensics provider confirmed that the log was likely accurate and reflected the exfiltrated data.
Affected individuals	The incident affected 1,519 individuals, including 82 individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	• Provided Alberta residents for whom there was a real risk of significant harm with one year of credit monitoring and identity theft insurance. • Conducted dark web monitoring to ensure that the compromised data was not published. • Provided interested clients with indicators of compromise and other incident-related facts that might help them avoid similar attacks. • Reset all passwords and implemented dual factor authentication. • Installed industry-leading end-point detection software to protect from repeat attacks. • Hired an IT security firm to review the cybersecurity program will make recommended improvements. • Notified the federal Office of the Privacy Commissioner. • Enhancing employee security training.
Steps taken to notify individuals of the incident	Affected employees were notified via email shortly after the incident. All affected individuals were notified by mail on December 7, 2020.
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 possible harms that may occur as a result of the breach are "Identity theft" and "Phishing". I agree with the Organization's assessment. A reasonable person would consider the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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.	The Organization reported, *The information ranges in sensitivity from very sensitive to innocuous. The information was accessed by a criminal ransomware syndicate, which raises the likelihood of misuse, despite the fact that [the Organization] obtained assurances of deletion. Consequently, depending on the weight given to those assurances of deletion, there is a low to moderate likelihood of harm. Out of an abundance of caution, [the Organization] has notified all residents of Alberta for whom there was a real risk of significant harm.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an

	unknown third party (deliberate intrusion, ransom demand). In this case, the information at issue was accessed and stolen. The information may have been accessible to the threat actors for over a week.

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 contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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 unknown third party (deliberate intrusion, ransom demand). In this case, the information at issue was accessed and stolen. The information may have been accessible to the threat actors for over a week.

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 mail on December 7, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner