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	PCL Constructors Inc. (Organization)
Decision number (file number)	P2020-ND-149 (File #015900)
Date notice received by OIPC	May 14, 2020
Date Organization last provided information	May 14, 2020
Date of decision	November 20, 2020
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 about current and former employees. • name, • address, • email address, • telephone number, • pay and withholding information, and • Social Insurance Number. 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 apples.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third party vendor, PaperlessPay Corporation (PPC), to provide its employees with electronic access to tax slips and pay stubs in PPC's database.

	• On February 20, 2020, the Organization received a notification from PPC that an unknown party had issued an advertisement purporting to sell access to PPC's database on the dark web. • On March 20, 2020, PPC confirmed that the threat actor had gained access to its database servers; the access occurred on February 18, 2020. • PPC's investigation did not determine what data had been accessed or viewed by the threat actor, if any.
Affected individuals	The incident affected 35,100 individuals of which 19,103 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• The Organization requested and confirmed that PPC removed all of the Organization's data from the database. • The Organization reported that PPC had advised that it shut down its database and is cooperating with the Department of Homeland Security (DHS) and the FBI. • Hired a forensic investigation firm to conduct a search of the dark web; no evidence of misuse of the Organization's personal information was found. • Offered credit monitoring and identity theft insurance to affected individuals for 12 months at no cost.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or mail on May 14, 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 access of personal information at issue, if it occurred, could potentially cause affected individuals to suffer from the harms of identity theft or financial fraud". In my view, a reasonable person would consider the contact, financial and identity information (Social Insurance Number) at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email address could be used for phishing, increasing 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 reported: *The likelihood that harm may occur to affected individuals …is moderate.* *PPC advised that it was the opinion of DHS and the FBI that the circumstances of the Incident are generally indicative of a threat actor who only reviews a database to determine its size and the number of records at issue, and not of a threat actor who accesses the personal information of individuals. However, while [the Organization] is not aware of any personal information of any affected individual being misused, PPC could not rule out that any particular part of the Database had been accessed by the threat actor, and therefore, cannot positively state that the threat actor did not access the personal information of affected individuals.* *The Incident was caused as a result of malicious intent, rather than a mistake, which increases the likelihood that harm could result to affected individuals.* *Of note, however, following the Incident, PCL hired a leading forensic investigation firm to conduct a search of the dark web in relation to the Incident, which advised that it found no evidence of misuse of PCL employees' personal information.* 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 an unknown third party (deliberate intrusion). The service provider, PPC, cannot positively state that the personal information was not accessed. Although the Organization reported that it has no evidence that the personal information at issue has been misused, identity theft and fraud can occur months and even years after a data 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 contact, financial and identity information (Social Insurance Number) at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email address could be used for phishing, increasing 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 unknown third party (deliberate intrusion). The service provider, PPC, cannot positively state that the personal information was not accessed.

Although the Organization reported that it has no evidence that the personal information at issue has been misused, identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individuals whose 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 email or mail on May 14, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner