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	Cognizant Technology Solutions Canada Inc. (Organization)
Decision number (file number)	P2020-ND-156 (File #016248)
Date notice received by OIPC	June 17, 2020
Date Organization last provided information	June 17, 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. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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: • employee's name on corporate credit card, card number, and expiry date in some instances; • name and financial information (for one employee). With the exception of corporate credit card information, 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	• The Organization reported that, on April 20, 2020, it was the victim of a ransomware attack carried out by international cyber criminals.

	• The Organization learned that the attackers staged and likely exfiltrated a limited amount of data from its systems. • Based on its investigation, this activity occurred between April 9 and 11, 2020.
Affected individuals	The incident affected 14 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Provided individuals with complimentary 12-month dark web monitoring services. • Cooperating with the FBI. • Improving overall security posture.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on June 17, 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated, *While we have no reason to believe that any fraudulent activity has been carried out on the accounts, to assist you, we are providing you with the following information about general steps you can take to protect against potential misuse of personal information. You should always remain vigilant, including by regularly reviewing your financial account statements. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. As a precaution, we have arranged for you, at your option, to enroll in a complimentary 12-month dark web monitoring service provided by ID Experts.* In my view, a reasonable person would consider the financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 "While we do not believe that this will create a risk of harm to our employees relating to this information, out of an abundance of caution we are notifying all of our employees who have active corporate credit card accounts". With respect to the individual whose financial information is at issue, the Organization reported "While we have not seen any public disclosure of the data and have no reason to believe it has been misused, we will also provide notice to this individual".

	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 and ransom demand). The Organization indicated it was likely that some data was exfiltrated from its systems. Further, the data may have been exposed for three (3) days.

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 financial information at issue could be used to cause the significant harms of identity theft and fraud. 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 and ransom demand). The Organization indicated it was likely that some data was exfiltrated from its systems. Further, the data may have been exposed for three (3) days.

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 the affected individuals in writing on June 17, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner