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	Accor Services Canada Inc. (the Organization)
Decision number (file number)	P2020-ND-095 (File #016410)
Date notice received by OIPC	July 9, 2020
Date Organization last provided information	July 9, 2020
Date of decision	September 3, 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: • name, • position/title, • mailing address, • residential / cell phone number, • social insurance number, • date of birth, • salary for each year employed, • bank account information, • citizenship, • hire date, and • termination date and garnishment information, if applicable. 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 March 18, 2020, the Organization's service provider, Ceridian Canada Ltd., became aware of suspicious activity on its network, and immediately launched an investigation. • On May 12, 2020, the service provider discovered a file containing personal information on a server that an unauthorized third party accessed on March 18, 2020 using a valid name and password of an active customer account. • On May 27, 2020, the service provider notified the Organization of the incident. • The service provider was unable to determine if the unauthorized third part viewed or exfiltrated the personal information at issue.
Affected individuals	The incident affected 1,038 former and current employees of the Organization who are residents in Alberta.
Steps taken to reduce risk of harm to individuals	The service provider: • investigated, • took servers off the network as a precaution, • disabled domain administrator accounts and recreated new accounts, • shut down remote access capability, • notified law enforcement authorities, • notified affected individuals, • offered credit monitoring and identity restoration assistance to affected individuals, • engaged external legal counsel, • implemented and updated various information security tools, • is monitoring inbound and outbound traffic from its systems.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on July 9, 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 "If the threat actor did indeed access this information, there is a risk that this information could be used to commit fraud, such as identity theft, against the affected individuals". In my view, a reasonable person would consider the contact, identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated, *Although Ceridian (the service provider) has no direct evidence that this file left the Ceridian network, we are notifying you because we cannot rule out that possibility.* 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 actions of an unknown third party. Although the Organization said there is "no direct evidence that the file left the Ceridian network", it was unable to determine if the unauthorized third part viewed or exfiltrated the personal information at issue.

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, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 actions of an unknown third party. Although the Organization said there is "no direct evidence that the file left the Ceridian network", it was unable to determine if the unauthorized third part viewed or exfiltrated the personal information at issue.

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 July 9, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner