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	McDonald's Restaurants of Canada Limited (Organization)
Decision number (file number)	P2017-ND-131 (File #005311)
Date notice received by OIPC	March 30, 2017
Date Organization last provided information	May 30, 2017
Date of decision	September 14, 2017
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 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, • email address, • telephone number, • employment background, and • other employment application information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In mid-March 2017, the Organization detected unusual activity on its web server environment that hosts the Canada Careers web application.

	• The Organization investigated and found that an unauthorized third party was able to upload malicious software via the web application to the web server, which then executed and allowed for remote connectivity. Once remotely connected, the unauthorized third party created a user account on the server and successfully downloaded a database export of the information contained in the Canada Careers web application. The incident is believed to have occurred on March 12, 2017. • Concerns were raised by alert mechanisms on March 13, 2017, but the full extent of the incident was not immediately known. • The Organization determined that those affected by the privacy breach applied online for a job with the Organization between March 2014 and March 2017.
Affected individuals	The incident affected 94,556 individuals, of which 4,919 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately took the affected servers offline and quarantined them in order to prevent further impact. • Investigated the root cause of the breach and took further steps to ensure this type of security breach does not happen again. • Offered free credit monitoring services, identity theft insurance and a dedicated call centre to address concerns and questions. • Notified every provincial and territorial privacy commissioner as well as the Office of the Privacy Commissioner of Canada. • Issued a press release about the incident.
Steps taken to notify individuals of the incident	• The Organization notified all affected individuals by mail during the first week of April, 2017. • If the mail was returned and the application form included an email address, the Organization then sent an email notification to those individuals.
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 that the harm was "unknown at the present time. However, based on the nature of the information, [the Organization] does not presently believe that significant harm is likely to result from the breach." In my view, the contact, employment and education information provide comprehensive profiles that could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing. 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 that the likelihood of harm is "unknown at the present time. However based on the nature of the information, (the Organization) does not presently believe that significant harm is likely to result from the breach. The investigation remains ongoing. At this time, (the Organization has) no information concerning the identity of the attacker, and therefore, the information has not been recovered." In my view, the likelihood of harm resulting in this case is increased because the incident resulted from malicious action of an unknown third party (deliberate intrusion and installation of malware). The information has not been recovered.

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.

The contact, employment and education information provide comprehensive profiles that could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing. These are significant harms. The likelihood of harm resulting in this case is increased because the incident resulted from malicious action of an unknown third party (deliberate intrusion and installation of malware). The information has not been recovered.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals in a letter in the first week of April 2017, and by email as necessary, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner