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	The Coca-Cola Company (Organization)
Decision number (file number)	P2018-ND-075 (File #008908)
Date notice received by OIPC	June 6, 2018
Date Organization last provided information	June 6, 2018
Date of decision	July 9, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the affected individuals 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 a Delaware-incorporated company with its headquarters in Atlanta, Georgia and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name and date of birth, or • name and social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported there were 5 affected individuals in Alberta; to the extent this information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 1, 2017, the Organization was informed by US law enforcement officials that a former US-based employee of a subsidiary of the Organization was found in possession of an external hard drive containing information that appeared to have been misappropriated from the Organization.

	• The precise date and time of the removal of the information from the Organization's premises is not known; however, the company believes that the former employee misappropriated the information prior to his separation from the company in August 2015.
Affected individuals	The Organization reported that "Of the affected individuals, five are residents of the Province of Alberta"
Steps taken to reduce risk of harm to individuals	• Recovered the records. • The former employee's credentials had been revoked upon separation from the company in 2015, preventing further access to the Organization's facilities or systems. • The suspect continues to be under investigation by US law enforcement authorities. • Cooperated with law enforcement officials in their investigation and undertook an internal review of the incident. • Will offer one year of free identity monitoring services to affected individuals.
Steps taken to notify individuals of the incident	The Organization reported that "At the request of the US Department of Justice, the Company delayed making any notifications regarding the incident in question, so as not to interfere with the ongoing criminal investigation. On May 9, 2018, the Company was informed by law enforcement officials that it could proceed to notify potentially affected individuals". The Organization said that it "will be mailing notifications to affected individuals in Alberta on June 4, 2018" and also that it is "…continuing to attempt to identify any other individuals whose PII may have been compromised during this incident, and will notify any other affected individuals as required as our investigation continues".
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 it "believes that only identity theft might be a real risk" and also that "The data elements at issue are of the type that, when combined with one or more other elements, which might be obtained from public sources like telephone directories, might be used to attempt to open accounts or obtain credit in the name of the individuals concerned". I agree with the Organization's assessment that the identity information at issue could be used to cause the significant harm of identity theft, as well as 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 that it "…does not consider that in the current circumstances, harm is likely to result to the individuals identified in the Records, but is providing this report and the proposed individual notifications out of an abundance of caution. …However, the Company notes that at this time, it does not have any information to suggest that the misappropriated information was used to commit identify theft. To the best of the Company's knowledge, all of the information in question was still in the possession of the Suspect, and all was recovered. ln addition, as noted above, only five individuals in Alberta appear to have been affected". In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (unauthorized access to the information and possible criminal activity as the suspect is currently under investigation). Although the Organization says that "to the best of [its] knowledge, all of the information in question was still in the possession of the Suspect, and all was recovered", it did not provide reasons why it believes this to be true. Further, the fact that there is no information at this time to suggest the information was used to commit identity theft does not preclude the information from being used for this purpose in the future.

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 as a result of this incident.

The identity information at issue could be used to cause the significant harm of identity theft, as well as fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (unauthorized access to the information and possible criminal activity as the suspect is currently under investigation). Although the Organization says that "to the best of [its] knowledge, all of the information in question was still in the possession of the Suspect, and all was recovered", it did not provide reasons why it believes this to be true. Further, the fact that there is no information at this time to suggest the information was used to commit identity theft does not preclude the information from being used for this purpose in the future.

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 reported that it "will be mailing notifications to affected individuals in Alberta on June 4, 2018". **I require the Organization to confirm, within 10 days of the date of this decision, that the affected individuals in Alberta have been notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner