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)	P2015-ND-14 (File #P2560)
Date notice received by OIPC	January 23, 2014
Date Organization last provided information	January 9, 2015
Date of decision	April 14, 2015
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 extra-provincial corporation, registered in Nova Scotia. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information related to the Organization's employees: • name • mailing address • Canadian driver's license numbers • Canadian passport numbers This information is "personal information" as defined in section 1(1)(k) of PIPA, and was collected from residents of Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	

Description of incident	• On December 10, 2013 the Organization discovered that one of its associates who was suspended pending the outcome of an investigation had stolen eight laptops that contained personal employee information. • The Organization informed law enforcement shortly after discovering the theft and recovered the missing laptops. • The Organization could not confirm if the personal information was actually used as a result of the theft. • The laptops were not encrypted.
Affected individuals	The number of affected individuals in Alberta was 73.
Steps taken to reduce risk of harm to individuals	The Organization has implemented a company-wide program to encrypt all laptops.The Canadian employees affected by this breach have been monitored by Equifax Canada and to date there has been no indication that fraud has occurred on their credit files.
Steps taken to notify individuals of the incident	The Organization notified all affected individuals on January 24, 2014 by letter.
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 it believes "the risk of identity-related fraud is remote." In my view, the personal information involved is of high sensitivity. It includes identifiers, such as Canadian driver's license and passport numbers. This information could be used to cause the harms of identity theft and fraud. In my view, 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 it has been working with law enforcement, and has recovered the laptops. It has no indication the information was misused and believes the risk of harm to individuals is remote. In my view, the likelihood of harm resulting from this incident is increased because the laptops were stolen, indicating malicious intent. While the laptops have been recovered, they were not encrypted and the Organization cannot confirm that the information was not accessed, further increasing the likelihood of harm.

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. In coming to this decision, I considered the following factors: the personal information at issue could be used to cause the significant harms of identity theft and/or financial fraud. The laptops were stolen, indicating malicious intent. While the laptops have been recovered, they were not encrypted and the Organization cannot confirm that the information was not accessed, further increasing the likelihood of harm. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals on January 24, 2014 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner