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	dōTERRA International LLC (Organization)
Decision number (file number)	P2016-ND-64 (File #002822)
Date notice received by OIPC	April 22, 2016
Date Organization last provided information	April 22, 2016
Date of decision	December 19, 2016
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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • Social Security Number (or equivalent), • payment card information (including full or partial card number, card security code and expiration date), • date of birth, • postal address, • email address, • telephone number, • username, and • passwords. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• A third-party vendor contracted by the Organization to provide data hosting and software services informed the Organization that an unauthorized intruder had accessed some of the third-party's systems. • The intrusion appeared to have resulted in the unauthorized acquisition in March 2016 of personal information of the Organization's customers. • An investigation into the incident revealed that not all the personal information stored on the server in question was encrypted.
Affected individuals	The incident affected 1,017 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered identity protection services to affected individuals for two years. • Reported the incident to law enforcement. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on April 18, 2016.
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 identify any specific harm that could result to affected individuals from this incident, but noted that it "has no indication at this time that the affected personal information has been used to commit fraud or identity theft." In my view, the personal information involved includes sensitive identity, financial, credential, and contact information that could be used to cause the harms of identity theft and fraud. 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 was not aware of any attempts to commit fraud or identity theft using the information obtained through this incident. However, due to the sensitivity of the personal information involved, the Organization considered that it should take steps to reduce the risk of harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization has not recovered 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. The personal information involved includes sensitive identity, financial, credential, and contact information that could be used to cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization has not recovered the personal information at issue. 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 by mail on April 18, 2016, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner