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	Arbonne International LLC (Organization)
Decision number (file number)	P2020-ND-148 (File #015942)
Date notice received by OIPC	May 28, 2020
Date Organization last provided information	May 28, 2020
Date of decision	November 17, 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 the 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 based in Irvine, California and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • first and last name, • email address, • mailing address, • order purchase history, • telephone number, and • account password. 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 April 20, 2020, the Organization discovered an unauthorized attempt to access its secure servers. • The Organization contained the attack, neutralized the threat, and assessed the impact of the incident.

	• The Organization determined the perpetrators accessed personal information on a single server, which contained personal information of its clients and independent consultants.
Affected individuals	The incident involved 2,951 Canadians, including 288 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reset password of the affected individuals. • Locked folder permissions on all web servers. • Setup a folder/file monitoring solution. • Setup Splunk alerts. • Performed internal vulnerability scan. • Validated all directories. • Cleared cache. • Identified and blocked all the source IP addresses. • Notified privacy regulators (Canada, B.C. UK, Poland, Puerto Rico, Australia, New Zealand)
Steps taken to notify individuals of the incident	Affected individuals were notified by email between May 22-24, 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 "The likely consequence might be identity theft, loss of control over their personal data, loss of confidentiality of personal data". I agree with the Organization's assessment. A reasonable person would consider the contact, transaction and credential information at issue could be used for identity theft and fraud, and to compromise other online accounts. Email addresses could be used for phishing, increasing affected individuals' vulnerability to 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 the likelihood that significant harm will result from this incident is "Very unlikely. The assessment is based on the level of sensitivity of the data. Only passwords are not publicly available data. However, all impacted passwords were automatically reset further to the discovery of the breach. Additionally, no payment card or government ID information was accessed". In my view, a reasonable person would consider the likelihood of harm is increased because the incident resulted from the malicious action of an unknown third party (deliberate intrusion), and a significant number of accounts were affected. The information was accessed by an unauthorized party and the Organization cannot

	know that the unauthorized party will not further use or disclose the information.

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 contact, transaction and credential information at issue could be used for identity theft and fraud, and to compromise other online accounts. Email addresses could be used for phishing, increasing affected individuals' vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm is increased because the incident resulted from the malicious action of an unknown third party (deliberate intrusion), and a significant number of accounts were affected. The information was accessed by an unauthorized party and the Organization cannot know that the unauthorized party will not further use or disclose the information.

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 by email between May 22-24, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner