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	Intex Recreation Corp. (Organization)
Decision number (file number)	P2017-ND-49 (File #005143)
Date notice received by OIPC	March 2, 2017
Date Organization last provided information	May 2, 2017
Date of decision	May 19, 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • email address, and • credit card information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On November 16, 2016, the Organization learned of the potential compromise of certain personal information of its customers.

	• The Organization immediately launched an investigation which found that unauthorized and malicious code may have been inserted into the company's website. • The incident occurred between approximately April 24, 2016 and December 14, 2016.
Affected individuals	There are 229 potentially affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a third-party forensic investigator to assist with the investigation. • Removed the malicious code, and rebuilt the website on a new server and added new protections. • Provided one year of identity restoration services at no cost to affected individuals and contact information for a person who can answer questions about the incident.
Steps taken to notify individuals of the incident	The Organization reported that it notified all potentially affected individuals on March 1, 2017.
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 did not specifically identify any harm that might result from this incident but reported that it is "notifying the potentially affected individuals" and is "providing information to help better protect against identity theft and fraud" as well as "one year of identity restoration services at no cost". In my view, the financial and contact information at issue could be used to cause the harms of identity theft, fraud and financial loss. In addition, email addresses could be used for phishing purposes. 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 did not provide its assessment of the likelihood of harm resulting from this incident but reported that it was "in the process of notifying the potentially affected individuals." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information may have been exposed for almost 8 months.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The financial and contact information at issue could be used to cause the harms of identity theft, fraud and financial loss. In addition, email addresses could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information may have been exposed for almost 8 months.	

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization notified affected individuals in Alberta on March 1, 2017, in accordance with the Regulation. The Organization is not required to notify affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner