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	LivingSocial Canada Enterprises Inc.
Decision number (file number)	P2013-ND- 31 (File #P2320)
Date notice received by OIPC	April 29, 2013
Date Organization last provided information	August 22, 2013
Date of decision	October 7, 2013
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 incorporated in British Columbia and registered to carry on business in Alberta. 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 a combination of the following information: • name, • email address, • hashed and salted passwords, • gender, • two unique identifiers used for internal purposes, and • date of birth (for one individual associated with Alberta). This information is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• Individuals register on the Organization's website to receive emails about consumer product, service or event information for a particular geographic location. • On April 12, 2013, the Organization became aware that an unauthorized intruder had used compromised credentials to hack into and extract information from the Organization's servers. • The compromised servers contained the above personal information, in addition to other information about terms of agreement, last preferred city, referral source, account information (last update and creation date) and default ID for credit card (not actual credit card number or information). • According to audit logs, unauthorized access occurred between April 2 and 12, 2013. • Individual information, including the personal information described above, appears to have been accessed and extracted from the servers sometime after April 10, 2013. • Investigation into the cause of the incident is continuing.
Affected individuals	• Several million individuals affected worldwide including 1.69 million Canadians. • Estimated 473,751 individuals associated with Alberta. • The Alberta affected individuals estimate is based on the number of individuals who last requested information for a location in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced password reset for all individual passwords. • Internal authentication requirements and monitoring practices enhanced. • Evaluation of and enhancement of security measures implemented in response to the incident. • Gap assessment ongoing.
Steps taken to notify individuals of the incident	• Email notification of the incident sent to all affected individuals, including Albertans, on April 26, 2013. • Notification and "Frequently Asked Questions" about identity theft and fraud protection posted on Organization website. Notification included caution with respect to receiving email purporting to be from the Organization and the risk of phishing.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 submitted it is widely accepted that names and email addresses are not sensitive forms of personal information. Only one Albertan's date of birth was involved. The Organization recognized that there is a possibility hashed and salted passwords could be reverse engineered given enough time and effort. The Organization did reference the harm of phishing in the email notification sent to affected individuals about the incident. In my view, the personal information involved in this incident is of low to moderate sensitivity. This information could be used to cause significant harm in the form of phishing, and with respect to the date of birth and possibly the use of passwords for other accounts used by affected individuals, identity theft or fraud. The Organization recognized in the email notification sent to the affected individuals about the incident the possible harm of phishing. 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 the containment and remediation steps taken by the Organization, in combination with the low sensitivity of the personal information involved, materially reduced the likelihood of significant harm occurring to the affected individuals in this circumstance. The Organization submitted the harm of phishing was speculative in these circumstances due to the containment and remediation efforts made by the Organization. The Organization forced a password reset. In addition, in four months since the incident, the Organization is not aware of any harm to the affected individuals as a result of this incident. The Organization, therefore, concluded that there is no real risk of significant harm to individuals affected by the incident. I agree that the steps taken following the incident reduced the risk of harm occurring. With respect to the hashed and salted passwords, in my view, the likelihood that significant harm could result from this incident is low due to the salting of the hashed passwords. However, there are factors involved that increase the likelihood that other harms will result from the incident. The incident involved a deliberate hack that is still under investigation. While the Organization has not received any report of phishing (unlike the circumstances in P2012-ND-09), this incident nonetheless involved a significant number of affected individuals which I have recognized in previous decisions as a factor that increases the risk of phishing occurring (P2013-ND-15).

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 incident involved a hack that is still being investigated. It also involved a large number of email addresses, which increases the risk of phishing. The affected individual whose personal information included a birth date is also at risk for identity theft or fraud. The passwords were protected to a degree with the hashing and salting, but it was recognized by the Organization that, given time, those could be reverse engineered. These factors contributed significantly to my decision. 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 in an email sent on April 26, 2013, which was in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner