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	Beachbody, LLC (Organization)
Decision number (file number)	P2013-ND-33 (File #P2332)
Date notice received by OIPC	May 29, 2013
Date Organization last provided information	July 8, 2013
Date of decision	December 13, 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 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 the following personal information: • name (first and last names), • email address, • mailing address, • telephone number, • credit card number, • credit card expiration date, and • credit card verification value number (CCV number). This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected from Alberta residents through the Organization's website.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• In March and April of 2013, several customers contacted the Organization to report that they experienced fraudulent charges on credit cards that had been used to make online purchases on the Organization's website. • The Organization hired forensic experts who confirmed that the Organization's website was hacked and the personal information may have been accessed by the hacker(s). • The forensic experts confirmed that credit card numbers and the corresponding expiry dates had been encrypted and were not stored in plain text. • Even though the credit card information was encrypted, the hacker(s) were able to access and obtain that customer information.
Affected individuals	Approximately 2300 customers were affected by this incident. Of these, 141 were Alberta residents.
Steps taken to reduce risk of harm to individuals	• The Organization reported the incident to the United States Secret Service. • A new secure website was created to replace the old website to prevent recurrence of a similar incident. • The Organization notified its payment processor of the incident. • A second forensic expert was hired to confirm the Organization's compliance with payment card industry standards. • All affected individuals were offered one year of free credit monitoring service.
Steps taken to notify individuals of the incident	• Email notifications were sent to affected individuals on May 10, 2013. A written letter notifying affected individuals of the incident was sent May 16, 2013. • A notice was posted on the Organization's website. • A confidential assistance telephone line was provided to all affected individuals who wished to speak to someone about their concerns or questions. • All email, written, and posted notifications outlined the nature of the incident, what personal information may have been compromised, and the steps that the Organization has taken to reduce the impact and recurrence of the incident.

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 recognized the affected individuals may be at risk for identity theft and fraud. In my view, the personal information involved is highly sensitive. It contains name, address, and credit card information. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. Further, there is a risk of phishing given the number of email addresses that were compromised. 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 due to the high sensitivity of the personal information involved, it considered there to be a real risk of significant harm to the affected individuals. In my view, there is a real risk of significant harm resulting from this incident. This incident involved a deliberate hack, perpetrated by unauthorized individuals with nefarious intent. The likelihood of harm resulting from this incident is increased because some customers reported fraudulent use of the credit cards that were used to make purchases on the Organization's website. Even though the credit card information was encrypted, it appears that the encryption was compromised.

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 involves sensitive identity information, such as name, address, and credit card information for all affected individuals. The information was hacked and some of the credit cards were used for fraudulent purposes. These factors contributed significantly to my decision. Although encrypted, it appears that the credit card information was used to cause 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 in an email dated, May 10, 2013, and in a letter dated May 16, 2013. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner