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	Aesop Canada Inc. (Organization)
Decision number (file number)	P2018-ND-34 (File #006567)
Date notice received by OIPC	September 14, 2017
Date Organization last provided information	September 14, 2017
Date of decision	February 28, 2018
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • shipping address, • telephone number, • email address, • account password, • credit card and debit card information (cardholder name, card number, expiry date, and security code). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• At the end of July 2017, one of the Organization's credit card issuers notified the Organization that it had noticed patterns of fraudulent transactions on credit cards that were used to purchase items from the Organization's website. • At the end of August 2017, the Organization discovered a web-form on its site that collected customer contact data and credit card numbers was altered to also send details to a third-party address. The skimming of this information was not authorized by the Organization. • The skimming appears to be a result of an application build weakness and it is not clear how the weakness was introduced to the application. • On August 31, 2017, the Organization decommissioned the infrastructure for the site to prevent further breaches. • The incident occurred between June 7, 2017 and August 31, 2017.
Affected individuals	The incident affected 388 individuals in Canada, including 40 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Decommissioned the infrastructure for the site which contained the compromised application effectively, halting any further leakage. • Hired an external forensic investigator to discover how the interception or unauthorized access occurred. • Will thoroughly test the replacement application to ensure the particular weakness responsible for this breach (and other potential weaknesses) are not present. • Will be launching a new website on a new platform. • Notified all credit card vendors • Notified law enforcement. • Notified all affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on September 8, 2017.
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 that "in light of the nature of the Customer Information there is a risk of misuse of the customer's financial information (e.g. credit card fraud), and the potential for fraud and identity theft…the card issuer noted unusual activity early and has identified the credit and debit cards involved in the incident, it is unlikely the harm will be significant. However, it acknowledges that under Alberta law, the Commissioner may characterize the attempts at credit card fraud as a potential significant harm."

	I agree with the Organization. The contact information and the financial information at issue (payment card numbers, security codes and expiry dates) could be used to cause the significant harms of identity theft and fraud. Email address could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.
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 of the harm noted above occurring was originally high but has diminished significantly. However, the Customer Information has not yet been recovered and [the Organization] and the forensic investigator have not been able to identify who is in possession of the information. [The Organization] has notified its affected customers and the card issuers are aware of the credit and debit cards involved so the opportunity for fraud has been decreased since the incident." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion) and the information had not been recovered. Even if credit issuers are aware of the incident, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 contact information and the financial information at issue (payment card numbers, security codes and expiry dates) could be used to cause the significant harms of identity theft and fraud. Email address could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion) and the information had not been recovered. Even if credit issuers are aware of the incident, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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

I understand the Organization notified affected individuals by email dated September 8, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner