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	BEL USA LLC (Organization)
Decision number (file number)	P2019-ND-106 (File #011498)
Date notice received by OIPC	December 31, 2018
Date Organization last provided information	December 31, 2018
Date of decision	July 19, 2019
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • email address, • telephone number, • credit card or debit 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 via the Organization's e-commerce website, DiscountMugs.com.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On November 16, 2018, the Organization discovered that an unauthorized change had been made to its DiscountMugs.com website.

	• The Organization investigated, and learned that unauthorized code was inserted into the shopping cart page designed to collect information customers entered on that page. • On December 20, 2018, the investigation determined that orders placed by credit or debit cards between August 5, 2018 and November 16, 2018, may have been impacted by the unauthorized code.
Affected individuals	The incident affected 70,244 individuals, including three (3) in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the unauthorized code. • Reported the matter to law enforcement and to the payment card companies. • Arranged for twelve months of identity repair and identity theft monitoring services for affected individuals, at no cost. • Hardened website design infrastructure and implemented additional intrusion detection monitoring to its systems. • Modified website to prevent reoccurrence.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 31, 2018.
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 did not specifically identify the harm(s) that might result from this incident, but its notification to affected individuals said "…we encourage you to remain vigilant for incidents of fraud on your payment card…". In my view, a reasonable person would consider that the contact and financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing 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 "There is no evidence at this time that any Alberta resident's personal information was in fact stolen as a result of this incident. Nevertheless, the payment card companies have been notified of this incident. Additionally, out of an abundance of caution, notice substantially similar to the attached is being provided to Alberta residents who placed an order through DiscountMugs.com between August 5, 2018 and November 16, 2018."

	In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and installment of malicious code. The personal information appears to have been exposed for over three months. Although the Organization reported there is no evidence that the personal information of Albertans was stolen, it did not report any evidence that the information was not exfiltrated (e.g. audit logs).

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 that the contact and financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion and installment of malicious code. The personal information appears to have been exposed for over three months. Although the Organization reported there is no evidence that the personal information of Albertans was stolen, it did not provide any evidence to confirm that the information was not exfiltrated (e.g. audit logs).

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 that affected individuals were notified by letter on December 31, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner