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	Costco US (Organization)
Decision number (file number)	P2016-ND-66 (File #001731)
Date notice received by OIPC	October 22, 2015
Date Organization last provided information	September 11, 2016
Date of decision	December 20, 2016
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 the State of Washington and operating in Alberta through its online presence. 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 some of the following information: • name, • telephone number, • billing address, • shipping information, • email address, • credit card information (including card security code and expiration date), and • password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization's third party photo services website provider suffered a security compromise on its website. • A forensic investigation revealed that malware had been active between June 19, 2014 and July 15, 2015 and only affected the US photo center website. • The Organization believes that the information of Canadian individuals who made purchases on the US photo center site may have been accessed by an unauthorized third party during this time. The Organization confirmed that image files uploaded by individuals were not affected.
Affected individuals	The incident affected approximately 1,000 Canadians, including 159 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified all affected customers. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada. • Offered free identity theft recovery and credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on September 21, 2015.
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.	In its report of the incident, the Organization did not specifically identify any harm that might result to affected individuals. However, its notice to affected individuals provides guidance should affected individuals "suspect fraudulent activity or if you would like to learn more about what to do if you suspect your identity has been stolen." In my view, some of the personal information at issue (contact) is of low sensitivity; however, credentials (passwords) and email addresses could be used to gain unauthorized access to other internet accounts and could be used to cause the significant harm of phishing. Credit card information (including card security code and expiration date) could be used to cause the significant harms of identity theft and fraud.
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 risk of harm to affected individuals. 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.

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. Some of the personal information at issue (contact) is of low sensitivity; however, credentials (passwords) and email addresses could be used to gain unauthorized access to other internet accounts and could be used to cause the significant harm of phishing. Credit card information (including card security code and expiration date) could be used to cause the significant harms of identity theft and fraud. 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. 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 a letter dated September 21, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner