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	Walmart Canada Corp. (Organization)
Decision number (file number)	P2017-ND-34 (File #001854)
Date notice received by OIPC	November 20, 2015
Date Organization last provided information	December 21, 2016
Date of decision	February 22, 2017
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 Nova Scotia and has its head office in Ontario. It operates in Alberta and 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, • email address, • credit card information (including 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 stored on a server in Ontario, and some was collected from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• One of the Organization's service providers suffered a security compromise on its website, which in turn affected the online services available to the Organization's customers. • A forensic investigation revealed that malware had been active between June 19, 2014 and July 15, 2015. • As a result, the Organization believes that its customers' personal information may have been accessed by an unauthorized third party during that time.
Affected individuals	• The Organization reported that approximately 109,000 Albertans transacted on the site during the relevant period.
Steps taken to reduce risk of harm to individuals	• Immediately shut down the website and initiated an investigation. • Notified all affected customers, posted a public website notice, and set up a 1-800 number to address customer questions. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on October 28, 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 notes that "We continue to encourage customers to contact their financial institutions if they suspect any irregular activity on their credit cards. We also recommend that you change the password you use on all other sites or services if it is the same password used for the photo site." In my view, 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, but as noted above, encouraged its customers to change their passwords, and to contact their financial institutions in case of suspicious transactions. 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 installation of malware). Further, the information may have been exposed for approximately 1 year.

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 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 (deliberate intrusion and installation of malware). Further, the information may have been exposed for approximately 1 year.

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 in an email dated October 28, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner