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	LÍLLÉbaby (Organization)
Decision number (file number)	P2018-ND-131 (File #009688)
Date notice received by OIPC	September 5, 2018
Date Organization last provided information	September 5, 2018
Date of decision	September 27, 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 whose 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 all or some of the following information: • name, • payment 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. To the extent the information was collected in Alberta via the Organization's e-commerce website, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In June of 2018, the Organization learned of a potential data security incident involving the unauthorized installation of malware on its e-commerce web platform. • It appears that payment card information may have been affected for customers who used the Organization's website from June 2016 until July 9, 2018.

Affected individuals	The incident affected 403 Canadians, including 57 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took immediate steps to secure payment card information. • Launched an investigation and retained a forensics firm to remove malicious code, determine what happened and whether customer payment card information had been accessed or acquired without authorization. • Reported the breach to the Federal Bureau of Investigation and payment card brands • Enhanced the security of the e-commerce platform and transitioned to processing payment cards in a way that bolsters transaction security. • Currently rebuilding the web platform to enhance security.
Steps taken to notify individuals of the incident	Affected individuals in Canada were notified by letter on August 28, 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's report of the breach did not specifically identify any harm(s) that might result from this incident, but its notification to affected individuals said that it had "reported the matter to the payment card brands in order to help prevent fraudulent activity" and also offered "identity monitoring services". In my view, the financial information at issue (payment card information) could be used to cause the significant harms of fraud, identity theft, financial loss and negative effects on a credit record.
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 "Given that [the Organization's] systems were affected by malware, and given the involvement of payment card information, [the Organization] is of the view that the test for mandatory breach reporting under the *Personal Information Protection Act* (Alberta) is met and that individual notification is required (as well as being the right thing to do)." 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 (malware), and the information may have been exposed for over two (2) years.
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 financial information at issue (payment card information) could be used to cause the significant harms of fraud, identity theft, financial loss and negative effects on a credit record. 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 (malware), and the information may have been exposed for over two (2) years.

The Organization is required to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that affected individuals in Canada were notified by letter on August 28, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner