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	Bombas, LLC (Organization)
Decision number (file number)	P2018-ND-125 (File #009632)
Date notice received by OIPC	September 4, 2018
Date Organization last provided information	September 4, 2018
Date of decision	September 26, 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, • address, and • credit card information. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization experienced a security incident on its website due to malicious code in its third party e-commerce platform used for payment card purchases.

	• The malicious code was initially identified and disabled from the website on January 15, 2015, and, after an inadvertent reintroduction, the malicious code was disabled on February 9, 2015, with remediation activities ending on February 25, 2015. • In the course of a 2018 review of its privacy and cybersecurity program, the incident was revisited, but, the Organization reported there is no definitive way to identify which transactions were impacted. • As the review of the incident has progressed, the Organization uncovered a copy of the code for the website at the relevant time, including the malicious code, and other evidence supporting the conclusion that the unauthorized access to personal information likely did not begin until September 27, 2014, at the earliest, and ran until, at the latest, the conclusion of remediation activities on February 25, 2015.
Affected individuals	The incident affected 39,561 individuals, including 245 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Conducted a privacy and data security program review, which has resulted in the development or enhancement of policies and training on reasonable and appropriate security measures designed to protect personal information, including by third party vendors and on managing data incidents. • Offered credit monitoring and identity theft protection services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letters sent May 21, 2018 and August 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 reported "Consumers are protected from direct financial loss if they report any fraudulent charges to their credit card companies. In some certain circumstances, it is possible that financial loss, fraud, or negative effects on a credit record may be possible." In my view, the financial information at issue (credit 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 assessed the likelihood of harm resulting from this incident as "Low: Although the information available included credit card information, payment card brands reimburse customers for fraudulent charges to their credit card and the card brands should have canceled the affected cards in 2015." 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 (malicious code), and the information may have been exposed for approximately five months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud or misuse. Even if this were the case, 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 financial information at issue (credit 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 (malicious code), and the information may have been exposed for approximately five months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud or misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 were notified by letters sent May 21, 2018 and August 31, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner