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)	P2021-ND-129 (File #016006)
Date notice received by OIPC	June 5, 2020
Date Organization last provided information	June 5, 2020
Date of decision	May 12, 2021
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 a US-based sock and clothier retailer and 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: • first and last name, • address, and • payment 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 at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In late January 2019, the Organization discovered that a malicious code had been uploaded onto its Shopify e-platform in order to scrape credit card numbers and other personal information. • The Organization determined that the malicious code was operating between November 11, 2016 and February 16, 2017.

	• The Organization's investigation determined that an unauthorized third party may have compromised the credentials of an employee's account in order to access the platform, and insert the malicious code. • The Organization can not rule out the possibility that the malicious code could have successfully scraped customer information. The Organization confirmed that a new security feature added to its e-commerce platform on February 16, 2017 prevented the code from functioning after that date.
Affected individuals	The incident affected 83,744 individuals, including 58 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Notified data protection regulators and other relevant authorities in Canada, the US, Australia and the UK. • Increased security on those accounts that access the Shopify platform. • Continues to actively monitor and develop its security processes and procedures.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 10, 2020.
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, *The malicious code could have enabled the attacker to acquire certain personal information belonging to customers who entered their payment card information on the e-commerce platform, with the potential for identity theft or fraud.* I agree with the Organization's assessment. A reasonable person would consider that the contact (name and address) and financial information at issue could be used to cause the harms of 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, *The incident occurred more than three years ago, and we are not aware of any theft or fraud being committed in respect of the potentially affected individuals, and such no incidents have been reported to [the Organization] or any other party with which it has a relationship in respect to this individual.* In my view, a reasonable person would consider 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, likely phishing). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately three (3) months.

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 (name and address) and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. 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, likely phishing). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately three (3) months.

I require the Organization 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 the Organization notified affected individuals by letter on June 10, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner