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	Mattress Insider LLC (Organization)
Decision number (file number)	P2020-ND-175 (File #016276)
Date notice received by OIPC	June 24, 2020
Date Organization last provided information	June 24, 2020
Date of decision	December 3, 2020
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 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 Colorado, U.S.A. organization and an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • email address, • billing address, • shipping address, • telephone number, • payment card data (account number, expiry date, security code). 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 via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure

Description of incident	• An unauthorized entity added malicious script to the Organization's payment gateway at mattressinsider.com. The script potentially sent payment card data to an unauthorized third-party website. • The breach was discovered on May 14, 2020 when the Organization was notified by its credit card acquirer, WorldPay, about fraudulent charges on cardholders' credit card accounts. • The Organization's investigation determined that the personal information may have been compromised between January 11, 2020 through May 14, 2020.
Affected individuals	The incident affected 1,708 individuals of which 2 are Albertans.
Steps taken to reduce risk of harm to individuals	• Identified and removed the extra code that was added to the compromised files which re-routed credit card information. • Searched server logs to identify additional threats. • Changed the payment gateway and check out module credentials for all staff. • Added additional monitoring to systems. • Terminated the business relationship with the payment gateway developers. • Continuing to assess and update security measures to safeguard the privacy and security of information and data. • Reported the incident to the FBI and filed a complaint with the Internet Crime Complaint Center. • Advised individuals to review credit card statements and monitor credit reports for suspicious activity. • Offered twelve months of complimentary credit monitoring with fraud alert and identity theft protection services/insurance.
Steps taken to notify individuals of the incident	Affected individuals were notified by direct mail on June 17, 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 "This incident involved potential unauthorized access to individual's name, address, payment card data, email address which could result in identity theft, financial harm and email scams/phishing". I agree with the Organization's assessment. A reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to 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 specifically provide an assessment of the likelihood of harm resulting from this incident, but reiterated that it could not know with certainty what data was compromised, and that it was notifying potentially affected individuals because their payment card data may have been subject to unauthorized access. 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, and the compromised information may have been exposed for 4 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 the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to 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, and the compromised information may have been exposed for 4 months.

I require the Organization to notify the affected individuals whose personal 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 direct mail on June 17, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner