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	Casper Sleep Inc. (Organization)
Decision number (file number)	P2018-ND-154 (File #009914)
Date notice received by OIPC	October 3, 2018
Date Organization last provided information	October 3, 2018
Date of decision	November 23, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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, • shipping address and instructions, • telephone number, • description of item(s) purchased, • payment card type and last four digits of payment card number, • billing address, and • email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization learned that a server containing customers' past order details could be accessed from the internet between May 5, 2016 and April 11, 2018. • The Organization investigated and found that the incident was caused by an error in the server configuration. • On July 12, 2018, Casper discovered that certain customer information may have been obtained by unauthorized individuals. • The impacted server contained information about orders customers placed between April 1, 2016 and May 5, 2016.
Affected individuals	The incident affected 158 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	• Took steps to address and contain the incident including taking the server offline, launching an internal investigation, and working with third party forensics. • Implemented a quarterly audit of web server configurations, hired an in-house Security Engineer, reviewed and modified the company's technical change management process, and plans to increase the scope of the company's bug bounty program to enhance the security of systems and networks. • Provided Alberta residents with a direct phone number and email address where affected individuals may reach out for additional information.
Steps taken to notify individuals of the incident	Canadian residents (including the affected Alberta residents) were notified via electronic mail on September 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 did not specifically identify any potential harm that might result from this incident but its notification to affected individuals provided information for customers to protect against "potential fraud or misuse of your information." In my view, a reasonable person would consider that the contact and profile (transaction) information, as well as email addresses, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm.

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 assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate, unauthorized access). Further, it appears the information was exposed for almost two 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 whose personal information was collected in Alberta.

A reasonable person would consider that the contact and profile (transaction) information, as well as email addresses, could be used for targeted phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate, unauthorized access). Further, it appears the information was exposed for almost two years.

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 Canadian residents (including the affected Alberta residents) were notified via electronic mail on September 28, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner