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	Claire's Store Inc. (Organization)
Decision number (file number)	P2021-ND-038 (File #016397)
Date notice received by OIPC	July 9, 2020
Date Organization last provided information	July 9, 2020
Date of decision	February 23, 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 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, • email address (only if a customer chose to edit their email on the checkout page), • telephone number, • payment card number, expiry date, and security code (for payment cards used for transactions while the unauthorized code was present.) • gift card number and PIN for gift cards (used for transactions while the unauthorized code was present could have also been copied), and • account password (but not email address, if a customer created an account during the checkout process). 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, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 11, 2020, the Organization was contacted by a security researcher who claimed the Organization's e-commerce site had been compromised. • The Organization investigated and identified and removed unauthorized code form its ecommerce site on Friday, June 12, 2020. • The code was capable of obtaining information entered by customers during the online checkout process and sending it out of the Organization's system. Purchases made in Organization's retail store locations were not involved. • The Organization reported that the code was first added on April 7, 2020. There were several times from April 7 to June 12 when the added code was not present because of new code deployments.
Affected individuals	The incident affected five (5) individuals in Canada, including two (2) residents in Alberta.
Steps taken to reduce risk of harm to individuals	• Advised individuals to closely review payment card account statements and immediately report any unauthorized charges to the bank that issued the card. • Provided a telephone number for individuals to call with any questions they may have. • Offered individuals who received a notification letter a complimentary one-year membership for internet surveillance and identity theft insurance at no cost. • Implemented additional security measures. • Notified the payment cards network and law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 8, 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, "It is possible that unauthorized charges could be made to involved payment cards." In my view, a reasonable person would consider that the contact and financial information at issue (including payment card numbers and expiry dates) 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 reported, *The likelihood of harm is very low. [The Organization] advised individuals to closely review payment card account statements and immediately report any unauthorized charges to the bank that issued the card. Payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported.* In my view, a reasonable person would consider that 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. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Finally, it appears the information was exposed for approximately 2 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 and financial information at issue (including payment card numbers and expiry dates) 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.

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. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Finally, it appears the information was exposed for approximately 2 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 the affected individuals by letter on July 8, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner