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	Defender Industries, Inc. (Organization)
Decision number (file number)	P2022-ND-012 (File #022191)
Date notice received by OIPC	July 14, 2021
Date Organization last provided information	July 14, 2021
Date of decision	March 31, 2022
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's head office is on Waterford, Connecticut, USA. 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 some or all of the following information: • names, • addresses, • credit card information, and • email addresses. 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	• On April 15, 2021, Defender became aware of malware on its e-commerce platform. • Defender submitted the breach occurred on November 22, 2020.

	• Defender took immediate steps to remove the malware and notified its merchant processor as well as Visa, Mastercard, and American Express. • On April 23, 2021, it was determined that this incident might involve personal information of certain Defender customers.
Affected individuals	The incident affected 803 Canadians, including 43 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Took immediate steps to remove the malware from e-commerce platform. • Notified payment card brands and credit reporting agencies. Notified payment card networks so that they can coordinate with card issuing banks to monitor for unauthorized activity on cards used during the identified timeframe. • Engaged an experienced payment card security firm to assist in securing the company platform. • Added software to prevent unauthorized changes to the platform. • Working on implementing an i-Frame solution to the processing of payment cards. • Provided information to affected individuals on how to obtain and monitor their credit history and protect personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on July 7, 2021.
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 possible harms that may occur as a result of the breach are, "A loss of credit card information and subsequent identity theft". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all 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, *…Payment card brands have been notified a [sic] of the event. Affected individuals have also been notified and have the opportunity to cancel their cards if requested. Affected individuals have been provided with information on how to obtain and monitor their credit history to minimize the risk of identity theft.*

	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). The Organization notified the payment card brands of the incident; however, affected individuals may be held responsible for any credit card fraud and misuse. As well, this action does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately 4 ½ 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 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). The Organization notified the payment card brands of the incident; however, affected individuals may still be held responsible for any credit card fraud and misuse. As well, this action does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately 4 ½ months.

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). The Organization notified the payment card brands of the incident; however, affected individuals may be held responsible for any credit card fraud and misuse. As well, this action does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately 4 ½ 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 email and letter on July 7, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner