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	Free Speech Systems, LLC (Organization)
Decision number (file number)	P2019-ND-079 (File #011229)
Date notice received by OIPC	December 14, 2018
Date Organization last provided information	December 14, 2018
Date of decision	June 24, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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: • name, • address, • email address, • password to e-commerce website, • order information, • payment card number, • card expiration date, and • card verification code. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected by the Organization via its e-commerce website. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On November 13, 2018, the Organization discovered unauthorized code on its website. • The unauthorized code was removed and an investigation was launched. • An investigation determined that the unauthorized code was added by an unauthorized individual so that payment card information entered by purchasers on the e-commerce website was copied and sent to an unauthorized server. • The code was added on November 12, 2018 and removed November 13, 2018.
Affected individuals	The incident affected 1,290 individuals, including one individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset affected individuals account password. • Provided an email address that individuals can contact if they have any questions. • Taking steps to improve its website security and moved to a more secure check-out method.
Steps taken to notify individuals of the incident	The affected individual was notified by email on December 14, 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 reported that "Unauthorized charges may be made to individuals' accounts." I agree with the Organization's assessment. A reasonable person would consider that the contact, credentials and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 that "Stolen payment card data is primarily used to make fraudulent charges. While card issuers' policies related to unauthorized charges may vary, payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Thus, potential harm is not likely to be significant". 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 (installation of an unauthorized code).

	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.

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 individual.

A reasonable person would consider that the contact, credentials and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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 (installation of an unauthorized code). 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.

I require the Organization to notify the affected individual 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 individual by email on December 14, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner