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	FastHealth Corporation (Organization)
Decision number (file number)	P2018-ND-021 (File #005781)
Date notice received by OIPC	June 1, 2017
Date Organization last provided information	November 30, 2017
Date of decision	January 31, 2018
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization develops and maintains operational platforms for a variety of business processes, including processing online bill payments on behalf of health care providers in the United States. The Organization is an "organization" as defined in section 1(1)(i) of PIPA and is reporting this incident on its own behalf.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • billing address, • email address, • telephone number, • payment card number, expiration date and security code (CVV), and • any comments or messages included with the payment. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via websites.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 21, 2016, the Organization identified suspicious code on a server, began an investigation and hired a computer security firm to assist. • On January 24, 2017, it was determined that an unauthorized third party altered code on the Organization's web server designed to capture payment card information as it was being entered on the online bill-pay platform from January 14, 2016 to December 20, 2016.
Affected individuals	The incident affected 4 Alberta residents who received services in the United States but provided the information at issue via website.
Steps taken to reduce risk of harm to individuals	• Immediately began an investigation and hired a computer security firm to assist in the investigation. • Removed the malicious code. • Notified affected health care providers. • Continues to take steps to strengthen security of its network.
Steps taken to notify individuals of the incident	In March 2017, the Organization started to identify affected individuals and in May 2017, began to obtain some of the affected individuals' contact information from health care providers. Affected individuals were notified by letter sent on May 26, 2017.
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 harm that might result from this incident includes "fraudulent purchases elsewhere online. However, the major credit card companies have rules that restrict them from requiring consumers to pay for fraudulent charges that are timely reported." In my view, the identity and financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the harms of identity theft, negative effects on credit reports and fraud. In addition, email address could be used to cause the harm of phishing. These are 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 "(g)iven that in Canada there is zero liability for fraudulent credit card purchases made on an individuals' credit card, there is no risk of significant harm to the affected individuals in Alberta arising from this incident. The affected individuals will be made whole by their credit card issuer. There may be inconvenience associated with the replacement cards, but that is not a significant harm."

	In my view, 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 and installation of malware). Further, the information may have been exposed for approximately one year. 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 individuals.

The identity and financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the harms of identity theft, negative effects on credit reports and fraud. In addition, email address could be used to cause the harm of phishing. These are 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 (deliberate intrusion and installation of malware). Further, the information may have been exposed for approximately one year.

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 individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in a letter on May 26, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner