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	Triple Flip Inc. (Organization)
Decision number (file number)	P2015-ND-48 (File #P2910)
Date notice received by OIPC	November 18, 2014
Date Organization last provided information	July 7, 2015
Date of decision	August 7, 2015
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 is registered in Alberta as an extra provincial corporation. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the information in question was collected from individuals residing in Alberta via an e-commerce website.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • phone number, • email address, • shipping and billing address, • account number, • expiry date, • card verification code (CVC), and • amount owed. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 15, 2014, the Organization's website suffered a cyberattack. • On October 20, 2014, malicious code was installed and infected a server. The code was designed to intercept the transmission of credit card and personal information. • On November 10, 2014 a customer reported their new credit card had been compromised. • The incident was investigated immediately and the website was shut down.
Affected individuals	• In total, 630 individuals were affected. • Of these, 230 Albertans were affected. • 55 Albertans reported their credit card had been used fraudulently.
Steps taken to reduce risk of harm to individuals	• All individuals were notified of the breach. • The website was immediately shut down. • All administrator passwords were changed. • Two-factor authentication was implemented. • Access is restricted to known Internet Protocol (IP) addresses. • New credit cards were issued. • Credit card protection was offered to all affected individuals.
Steps taken to notify individuals of the incident	Notification was made by email on November 14, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 concluded the information could be used for identity theft or fraud. I agree with the Organization. The personal information involved is highly sensitive. It contains name, email address, shipping/billing address and credit card information. The types of harm that could result from the unauthorized access are identity theft and fraud. In my view, 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 there was a high risk that the information could be used for criminal purposes. I agree there is a real risk of significant harm in this case since the incident was the result of malicious intent. Some of the affected individuals have already experienced 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 there is a real risk of significant harm as a result of this incident. The personal information at issue could be used to cause the significant harms of identity theft and fraud. The incident was the result of malicious intent and a number of affected individuals have already experienced 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 the affected individuals by email on November 14, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner