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	North 40 Outfitters (Organization)
Decision number (file number)	P2019-ND-103 (File #012361)
Date notice received by OIPC	February 28, 2019
Date Organization last provided information	February 28, 2019
Date of decision	July 17, 2019
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: • name, • credit or debit card number, expiry date, and security number or CVV. The Organization also reported that "…user account names and passwords may also have been affected". This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about November 8, 2018, the Organization identified suspicious activity regarding its online payment processing platform.

	• On or about December 14, 2018, the Organization's forensic investigation determined that customer credit and debit card information for transactions that occurred on its e-commerce website between February 2, 2018 and November 20, 2018 may have been subject to unauthorized access and/or acquisition.
Affected individuals	The incident affected three individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and retained a third party forensic firm. • Working to implement additional safeguards and training for employees. • Continuing to monitor the e-commerce environment to guard against suspicious activity. • Reported incident to credit card companies and notified data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about February 14, 2019.
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 did not specifically identify potential harms that might result from the incident but reported that it "…is providing all impacted individuals with guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause identity theft and fraud. Credentials (user account names and passwords) could be used to compromise other online accounts. 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 did not specify the likelihood of harm resulting from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion by an unknown third party. The personal information may have been exposed for almost 10 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 financial information at issue (including credit card number, expiry dates, and security codes) could be used to cause identity theft and fraud. Credentials (user account names and passwords) could be used to compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion by an unknown third party. The personal information may have been exposed for almost 10 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 or about February 14, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner