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	Tommie Copper Inc. (Organization)
Decision number (file number)	P2018-ND-064 (File #006872)
Date notice received by OIPC	October 16, 2017
Date Organization last provided information	October 31, 2017
Date of decision	July 3, 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • billing address, • full credit card number, • expiration date, and • CVV number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or around August 11, 2017, the Organization was advised that it had been identified as a common point of purchase for potential credit card fraud.

	• The Organization's forensic investigator determined that malware had been inserted into the Organization's website that collected certain payment information used at the checkout. • The Organization discovered that payment card information used by customers at its website was subject to unauthorized access from April 25, 2017 through August 29, 2017.
Affected individuals	The incident affected 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately launched an internal investigation. • Hired a third party forensic investigator. • Removed the malicious code from the affected system. • Took additional steps to ensure the security of its system. • Providing guidance to customers on how to better protect against identity theft and fraud, obtain a free credit check, and place a fraud alert and security freeze on one's credit file.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 6, 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated "You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* which includes guidance on steps you can take to better protect against the possibility of fraud and identity theft." In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss.
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 specifically provide an assessment of the likelihood that significant harm would result from this incident 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 four 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.	

The financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. 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 four months.

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 letter October 6, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner