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-094 (File #009229)
Date notice received by OIPC	July 18, 2018
Date Organization last provided information	July 18, 2018
Date of decision	August 1, 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 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 all or some of the following information: • name, • address, • telephone number, • email address, • payment card number, expiry 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	• The Organization was contacted by representatives of the credit card industry regarding potential fraud related to credit cards used on the Organization's website.

	• The Organization investigated and, on or about June 1, 2018, confirmed that a piece of malware had been inserted into the Organization's website that collected payment information used at checkout. • Certain payment information used by customers on the website was subject to unauthorized access from November 10, 2017 through January 5, 2018 and from January 21 to January 22, 2018.
Affected individuals	The incident affected 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Retained a third party forensic investigator. • Enhanced the security of the information stored on its systems, including more rigorous review of changes made to its code base, limiting the number of individuals with access to website administrative console, whitelisting IP addresses, strengthening requirements for system passwords, and reviewing the User Audit Report daily. • Notified state regulators and credit reporting agencies.
Steps taken to notify individuals of the incident	On July 11, 2018 the Organization began mailing written notification of the incident to affected individuals.
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 "We are providing notice of this incident to those who may be impacted so that they can take steps to prevent against possible fraud…". In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the harms of fraud, identity theft and financial loss. Email addresses could be used for phishing purposes. 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 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 over 2 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 harms of fraud, identity theft and financial loss. Email addresses could be used for phishing purposes. 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 (deliberate intrusion and installation of malware). Further, the information may have been exposed for over 2 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 on July 11, 2018 the Organization began mailing written notification of the incident to affected individuals. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner