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	Carbon Environmental Boutique Ltd. (Organization)
Decision number (file number)	P2018-ND-065 (File #005833)
Date notice received by OIPC	June 13, 2017
Date Organization last provided information	June 13, 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 operates in Alberta and 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, • email address, • telephone number, • order/registration information (what was ordered, how much, etc.), and • credit card information (name, number, expiry). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On May 5, 2017, the Organization learned that its website hosting server was compromised.

	• The incident was investigated by the Organization's website and hosting provider, Pixel Army. The investigation found evidence that credit card information was compromised (skimmed in real time). • The website was compromised between October 20, 2016 and May 5, 2017.
Affected individuals	The incident affected 26 individuals.
Steps taken to reduce risk of harm to individuals	• Locked down the existing server. • Built a new server. • Scanned for malicious code and files. • Migrated over to the new server. • Implemented additional server security. • Not processing online payments once website is relaunched.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent on May 17, 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 the incident was "intercepted credit card information". In my view, the financial information at issue (credit card information) could be used to cause the significant harms of identity theft and fraud. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.
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 "Yes there is evidence of hacking, malware and theft" and "Yes the information can be used for criminal purposes". Further, the Organization said "26 potential customers were compromised. While none of the customers have notified us indicating they had a problem, we are still taking this seriously." 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 six 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 (credit card information) could be used to cause the significant harms of identity theft and fraud. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. 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 six 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 a letter on May 17, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner