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	Atlantic Cigar Company, LLC (Organization)
Decision number (file number)	P2017-ND-148 (File #006875)
Date notice received by OIPC	October 17, 2017
Date Organization last provided information	October 17, 2017
Date of decision	November 7, 2017
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 the following information: • name, • postal address, • email address, and • payment card data including credit card number, expiry date, and card verification number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta (e.g. via ecommerce website) I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 25, 2017, the Organization was notified by its service provider, Aptos, that an unauthorized third party accessed payment card information of 26 residents of Alberta stored on Aptos' systems. • The service provider reported to the Organization that the security incident lasted from July 21, 2017 to August 9, 2017.
Affected individuals	The incident affected 26 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged a cybersecurity firm to remediate the incident. • Reported the incident to law enforcement.
Steps taken to notify individuals of the incident	The Organization reported that it will notify affected individuals beginning October 11, 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 could result from the incident but reported that it would "provide 12 months of credit monitoring and identity protection services to affected consumers". Further, the Organization's notice to affected individuals recommended they "promptly report any fraudulent activity or any suspected incidence of identity theft" to law enforcement. In my view, the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes. 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.	In its report of the incident, the Organization did not specify the likelihood that harm to affected individuals could result. 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). Further, the information appears to have been exposed for almost three weeks.
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 could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes. These are 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). Further, the information appears to have been exposed for almost three weeks.

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).

In its report of the incident, the Organization said that it would notify affected individuals beginning October 11, 2017. I require the Organization to confirm to my office within 10 days of this decision that it has notified affected individuals in Alberta in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner