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	DirectVapor, Inc. (Organization)
Decision number (file number)	P2021-ND-196 (File #018794)
Date notice received by OIPC	December 21, 2020
Date Organization last provided information	December 21, 2020
Date of decision	October 15, 2021
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 headquartered in Florida, USA and is an ecommerce entity that sells, among other things, vaporizer pens and E-Cigarettes. 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 some or all of following information: • customer name, • credit or debit card number, including expiry date, and security code or card verification code. 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, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 23, 2020, the Organization became aware of suspicious activity associated with its online checkout page.

	• The Organization investigated and determined that an unauthorized user had gained access to its online payment platform and payment card information entered between September 14, 2020 through September 23, 2020.
Affected individuals	The incident affected 10,544 individuals, including three (3) Alberta residents.
Steps taken to reduce risk of harm to individuals	• Fixed the vulnerability. • Audited systems. • Installed additional controls to enhance system security. • Implemented multi-factor authentication for remote access. • Notified data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 21, 2020.
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 "…there is a real risk of significant harm to the affected individuals (i.e. risk of financial harm) as a result of the threat actor accessing the above noted information." In my view, a reasonable person would consider that the contact (name and address) and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 reported that it "determined there was a real risk of significant harm to the affected individuals..." In my view, a reasonable person would consider 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 may have been exposed for approximately ten (10) days.
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 contact (name and address) and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 may have been exposed for approximately ten (10) days.

I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on December 21, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner