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	KandyPens Inc. (Organization)
Decision number (file number)	P2020-ND-187 (File #016315)
Date notice received by OIPC	June 25, 2020
Date Organization last provided information	June 25, 2020
Date of decision	December 16, 2020
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 an e-commerce entity that sells vape pens and vaporizer pens. The Organization is located in California, USA, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue may have included: • name, • credit or debit card number, expiry date and security/verification code. 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 online payment platform.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In January 2020, the Organization became aware of suspicious activity associated with the online payment process for its e-commerce platform.

	• An investigation determined that an unauthorized user gained access to the Organization's online payment platform and credit and debit card information entered between March 7, 2019 and February 13, 2020 may have been compromised.
Affected individuals	The incident affected 1,324 individuals in Canada, including 199 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	• Remediated the vulnerability on the website. • Increased monitoring of the online payment system. • Recommended affected individuals review their credit and debit card statements for cards used on the Organization's website between March 7, 2019 and February 13, 2020. • Arranged for a call center with a designated toll free number for affected individuals to call for further information. • Reported incident to major credit card companies and responded to inquiries by the credit card brands. • Notified various state regulatory agencies. • Implemented file integrity monitoring. • Updated and created new policies and procedures to protect the security and privacy of customer information. • Implemented daily security vulnerability and malware scans and weekly scans of website and database. • Increased server access log retention period to one year. • Implemented content security policy.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 24, 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 it "… has determined that there is a real risk of significant harm to the affected individuals (i.e. the risk of financial harm) as a result of the threat actor redirecting the above noted information to a different, fraudulent website." In my view, a reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. 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	The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident. However, its notification to individuals stated: *You should carefully review the credit and debit card statements for any cards used on our website between March 7, 2019 and February 13, 2020. If you identify any suspicious*

between the incident and the possible harm.	*activity, you should immediately contact your financial institution.* 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 eleven (11) 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.

A reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. 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 eleven (11) months.

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 June 24, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner