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	Aurora Cannabis Enterprises Inc. (Organization)
Decision number (file number)	P2021-ND-009 (File #018844)
Date notice received by OIPC	January 4, 2021
Date Organization last provided information	January 26, 2021
Date of decision	February 16, 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 those 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 "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[1]: • name, • email address, • mailing address, • telephone number, • order information, • credentials, • bank account information, • pay statements, • credit card information, • passports, • driver's licenses, • national card, • social insurance number, • immigration application, • work visa information, • citizenship information, • student identification,

[1] Personal information involved varied by individual.

	• benefits information, • health card information, • drug card information, • health information, and • resumes. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between December 24 and December 26, 2020, the Organization was subject to a cyberattack involving unauthorized access to its SharePoint environment. • The incident was discovered on December 25, 2020, when a threat actor contacted the Organization, claiming to have hacked into the Organization's system. • Upon investigating, the Organization found that the incident resulted from use of credentials that a third party service provider included in an email. • The Organization uses a third party service provider who had an employee working on a project for the Organization at the time of the breach. The third party indicated that an employee's account names and passwords were uploaded in plaintext to a public repository. • On January 14, 2021, the Organization confirmed the threat actor had exfiltrated personal information and made the records publicly available on the dark web. • The Organization did not report attempting to remove the compromised records from the dark web.
Affected individuals	The incident affected 155 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated the issue. • Reported the incident to police. • Mandated training for all employees and service providers to protect against reoccurrence of a similar incident. • Offered credit and dark web monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or registered mail between December 31, 2020 and January 15, 2021.

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 potential harm(s) vary depending upon the type of information impacted for each individual. For example, individuals whose email addresses were impacted may be at risk of phishing. Individuals whose financial information were impacted may be at risk of financial harms such as theft or fraud. The customers whose information was impacted may also be at risk of non-financial harms, such as embarrasment [sic.].* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, financial, and employment information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Individuals may also experience the harms of embarrassment, and loss of employment or business opportunities. 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: *Based on the nature of the incident, the risk of phishing attempts, theft and fraud is high, for individuals where the information compromised would allow for such harms. The Organization asseses [sic.] the risk of embarrasment [sic.] related to the impacted customers as low, given that the Organization only collects information from certain customers in order to verify identity, without collecting any additional information from which another person can draw context.* 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 extraction of information). Despite the Organization's view that risk to customers is low, personal information used to verify a customer's identity remains compromised and a lack of "additional information from which another person can draw context" does not mitigate against future harms occurring. Further, the Organization did not attempt to remove the records from the dark web where they have been made publicly available by the threat actor.

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, identity, financial, and employment information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Individuals may also experience the harms of embarrassment, and loss of employment or business opportunities. 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 and extraction of information). Despite the Organization's view that risk to customers is low, personal information used to verify a customer's identity remains compromised and a lack of "additional information from which another person can draw context" does not mitigate against future harms occurring. Further, the Organization did not attempt to remove the records from the dark web where they have been made publicly available by the threat actor. I require the Organization to notify the affected individuals whose personal 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 or registered mail between December 31, 2020 and January 15, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner