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	Canopy Growth Corporation (Organization)
Decision number (file number)	P2018-ND-109 (File #009397)
Date notice received by OIPC	August 9, 2018
Date Organization last provided information	August 9, 2018
Date of decision	August 13, 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 the individuals whose 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 information that may have been compromised varies but includes some or all of the following: • name, • email address, • telephone number, • city of residence, and • answers to survey questions related to cannabis usage, interest in the Organization's products post legalization and interest in attending the Organization's sponsored events. 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	• The Organization uses a third party service provider, Typeform S.L. (a Barcelona-based online software as a service company), to collect marketing data. • The Organization reported that "on June 22, 2018", Typeform informed the Organization that "On June 27, 2018, our engineering team discovered that an unknown third party gained access to our server and downloaded certain information, including some of the data your respondents provided via Typeform." • The Organization said that subsequently, on July 11, 2018, Typeform informed it that "From the initial analysis from the forensic company, there are indications of compromise on one of our servers that shows continuous attempts to exploit the application layer. This appears to have allowed the attacker to retrieve an AWS API key from the server." • The Organization was advised by Typeform that "an unidentified attacker gained access to partial database backups stored in a private AWS S3 bucket" on June 22, 2018 and on June 25, 2018. • The Organization "was advised that over 233,000 Typeform accounts were compromised…".
Affected individuals	The Organization reported it was advised that 18 residents of Alberta were affected.
Steps taken to reduce risk of harm to individuals	The Organization reported that Typeform advised: *We have immediately initiated a comprehensive review of our system security and have identified the source of the breach and have addressed that security vulnerability .... we brought in forensic security experts who have helped us review the breach, and are helping us look into all other aspects where we can improve the security of our platform .... Regarding this specific incident, we've identified the vulnerability and implemented measures to prevent this type of attack .... We will continue to take significant measures to prevent this type of situation from happening in the future, including a full-scale review of our security.*
Steps taken to notify individuals of the incident	The Organization reported that it notified the affected individuals in Alberta by email on August 3, 2018.

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 that "An unauthorized persons [sic] could use the personal information of the 18 Albertans to engage in a phishing exercise. With respect to the 3 Albertans who provided additional information, an unauthorized person could use the information to humiliate, embarrass or blackmail said individuals. It could also potentially result in a loss of relationship, employment or business opportunity." I agree with the Organization's assessment. In my view, a reasonable person would consider that the email addresses on their own, but particularly when combined with profile information (survey responses and connection to the Organization), could be used for phishing purposes, as well as to humiliate or embarrass individuals, or cause harm to personal or employment relationships. These are all 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: *At the outset, we note that the affected 18 individual's personal information is "buried" among, what [the Organization] imagines, is the personal information of millions of affected individuals around the world. Again, [the Organization's] account was one of over 233,000 Typeform accounts that were compromised. As such, the likelihood of an unauthorized person finding such data "in the haystack" of personal information seems remote. In addition, the company's surverys [sic] were adult-directed, so there is no potential harm to minors. [The Organization] does not have information as to whether any other vulnerable individuals, such as seniors, may have been affected. Based on the foregoing, it would appear that the likelihood of harm would be low.* *That said, neither [the Organization] nor Typeform appear to know who accessed the data without authority. As a result, [the Organization] has assumed that such an actor has done so for malevolent purposes. Moreover, some of the information that was accessed could be deemed to be sensitive. In addition, it appears that the information was unencrypted. Finally, [the Organization] is currently unaware whether any of the applicable personal information has been recovered.*

	As a result, [the Organization] has taken the conservative position (out of an abundance of caution) that there is a reasonable likelihood of harm, particularly with respect to 3 Albertans who disclosed additional personal information. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was not encrypted and was compromised due to deliberate malicious action (cyber-attack). It appears the information may have been the target of the cyber-attack. The Organization has not identified the perpetrators, and information was downloaded and has not been recovered. The information was accessed on two separate occasions.

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 email addresses on their own, but particularly when combined with profile information (survey responses and connection to the Organization), could be used for phishing purposes, as well as to humiliate or embarrass individuals, or cause harm to personal or employment relationships. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was not encrypted and was compromised due to deliberate malicious action (cyber-attack). It appears the information may have been the target of the cyber-attack. The Organization has not identified the perpetrators, and information was downloaded and has not been recovered. The information was accessed on two separate occasions.

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 that the Organization notified the affected individuals in Alberta by email on August 3, 2018. The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner