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	Beakerhead Creative Society (Organization)
Decision number (file number)	P2020-ND-008 (File #013738)
Date notice received by OIPC	October 18, 2019
Date Organization last provided information	October 18, 2019
Date of decision	February 11, 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 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"	PIPA applies to "non-profit organizations" as defined in PIPA, but only to the extent the non-profit collects, uses or discloses personal information in connection with a commercial activity. In this case, the Organization says it is a non-profit organization as defined in PIPA, and it reported this incident "…in the context of its collection and use of personal information to sell tickets to [the annual festival staged by the Organization], and as a precaution given that this activity may qualify as "commercial activity" within the meaning of PIPA". To the extent the personal information at issue was collected, used and/or disclosed in connection with commercial activities, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved email addresses registered to receive communications from the Organization, including information about advance ticket sales to the Organization's 2020 Festival (the "Advance Ticket List"). To the extent this information is about identifiable individuals (as opposed to a generic business email account, for example), it is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization maintains several email distribution lists for purposes which include promoting the Organization's annual festival. • The email distribution list is managed through a third party, online email management service provider (the Service), which requires users to login to an account using a username and password. Once logged in, a user can access, export, and download a spreadsheet of a specific email distribution list from the Service. • On the afternoon of October 1, 2019, the Organization received an automated email alert from the Service which stated that a specific email distribution list had been exported and downloaded. • As the account activity and internet protocol (IP) address described in the alert were not immediately recognizable, the Organization investigated to determine whether there had been any unauthorized access to personal information under its control. The Organization was not able to conclusively determine that the export and download was made by authorized personnel.
Affected individuals	The incident affected approximately 3,819 distinct email addresses.
Steps taken to reduce risk of harm to individuals	• Contacted the Service and locked down its account pending a review of account activity. • Changed login information for the Organization's accounts to prevent any further potential unauthorized access. • Investigated and confirmed the personal information at issue. • Interviewed staff to determine whether the unrecognized account activity was authorized, but could not confirm. • Changing account login credentials, and obtaining individualized login credentials for all authorized personnel. • Monitoring account activity for any other unrecognized activities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email.

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 "This incident presents a real risk of significant harm to the affected individuals. There may be an increased risk of unsolicited emails, phishing scams, or SPAM emails to affected individuals". In my view, a reasonable person would consider that the email addresses at issue, and the known relationship with the Organization, could be used to cause the harm of phishing, resulting in increased vulnerability to identity theft and fraud.
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.	As noted above, the Organization reported "There may be an increased risk of unsolicited emails, phishing scams, or SPAM emails to affected individuals". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the Organization is unable to confirm the cause of this breach, suggesting it was the result of deliberate, possibly malicious, unauthorized action.

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 at issue, and the known relationship with the Organization, could be used to cause the harm of phishing, resulting in increased vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the Organization is unable to confirm the cause of this breach, suggesting it was the result of deliberate, possibly malicious, unauthorized action.

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 affected individuals were notified by email. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner