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	Francis Winspear Centre for Music (Organization)
Decision number (file number)	P2021-ND-126 (File #018202)
Date notice received by OIPC	November 19, 2020
Date Organization last provided information	March 30, 2021
Date of decision	May 11, 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 reported that it is incorporated under Alberta's *Companies Act* and therefore is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. The Organization says "The information was collected by the organizations from vendors and service providers in the course of each organization's core non-profit and charitable activities". To the extent the personal information at issue was collected, used and disclosed by the Organization in connection with commercial activities, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • organization, • address, • email address, • telephone number, • social insurance number (for 79 individuals),

	• ID number created for the vendor/service provider, • last invoice information, and • balance due to the vendor/service provider. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. According to the Organization, some of the information is business contact information for representatives of organizations. "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Blackbaud is a third party service provider to the Organization. The Organization uses Blackbaud's financial management tools (Financial Edge) to manage invoicing data relating to vendors and service providers. • According to Blackbaud, an intruder had access to some of Blackbaud's systems from about February 7, 2020 to May 20, 2020 and was able to extract backup data relating to the Organization. The intruder obtained access through another Blackbaud customer's account and then launched an attack.
Affected individuals	The Organization reported the incident in conjunction with another organization, and reported 498 individuals in total were affected.

Steps taken to reduce risk of harm to individuals	The Organization reported that its service provider: • Detected the intrusion, blocked further access, and commenced an investigation. • Retained third party forensic investigators and involved U.S. law enforcement (FBI). • Paid the demand for ransom so that the intruder would destroy all copies of the data and has received assurances that the data has been destroyed and was not shared with other third parties. • Is engaged in ongoing monitoring of dark web for data dumps in whole or part that contain the Organization's data. The Organization: • Provided notice to affected individuals and offered 24 month complimentary credit monitoring services to individuals whose social insurance number were included. • Removed social insurance numbers from Financial Edge. • Is currently evaluating Blackbaud's remedial activities.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter, email, and/or telephone between November 16 and November 27, 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: *For the 79 individuals whose social insurance numbers were exposed, the risk of harm could include fraud and identity theft. Some of the affected individuals may be at risk of phishing if the information included a phone or email address. While those individuals whose information only included a mailing address may be less susceptible to phishing, it is theoretically possible that a motivated person could learn other information about them, such as through LinkedIn or other social media, and combine this information to conduct phishing.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to 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 between the incident and the possible harm.	The Organization reported: *Based on Blackbaud's representations, the risk would appear to be less than probable and possibly low. However, there is no way to verify that the data has been destroyed and the organizations are not privy to the forensic investigation reports of Blackbaud. Accordingly, the organizations are unable to assess the strength of the likelihood that the data has been destroyed.* *Therefore, in assessing risk in these circumstances, the organization has given more weight to the malicious nature of the attack and concluded that there remains a non-speculative risk of significant harm.* I agree with the Organization's assessment that a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

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, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). Although Blackbaud reported it has no reason to believe that any data was or will be misused, the Organization cannot rule out this possibility.

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, letter, and telephone from November 16-27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner