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	Relevant Radio (Organization)
Decision number (file number)	P2019-ND-124 (File #019521)
Date notice received by OIPC	February 19, 2021
Date Organization last provided information	February 19, 2021
Date of decision	April 27, 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 a radio network based in Green Bay, Wisconsin and 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: • name, • address, • email address, • telephone number, • gender, and • spouse's name. 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	• The Organization uses Blackbaud, a third-party cloud computing vendor, to provide customer relationship management and financial services tools.

	• On July 16, 2020, Blackbaud informed the Organization that it had suffered a cyber incident which resulted in a potential unauthorized access to certain information maintained by Blackbaud between February 7, 2020 and May 20, 2020. • Blackbaud paid the threat actors' ransom demand in return for confirmation that all data removed by the threat actors had been destroyed.
Affected individuals	The incident affected 43 Alberta residents.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Notified law enforcement. • Is working with forensic experts to investigate the incident. • Engaged a third party to monitor the dark web to ensure no misuse of the accessed data. The Organization: • Commenced an investigation to determine what information was potentially at risk, to whom it relates, and address where each potentially impacted individual could be reached for notification. • Notified affected individuals and advised them to be vigilant in monitoring emails and credit reports. • Provided affected individuals with a document entitled "*Steps You Can Take to Protect Personal Information".* • Is reviewing its existing policies and procedures regarding third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter or email on February 17, 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 that while it "…assesses the risk of harm as low, affected individuals may be subject to phishing attempts or unsolicited communications." In my view, a reasonable person would consider that the contact information particularly in combination with email addresses and other profile information (gender, association with the Organization), could be used for the purposes of 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: *Risk of harm is assessed as low. Threat actors confirmed that the compromised data had been destroyed. Additionally, Blackbaud and third parties have monitored the Dark Web and no instances of release, misuse or dissemination of Blackbaud's data (or [the Organization's] data) has been observed.* In my view, 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 information particularly in combination with email addresses and other profile information (gender, association with the Organization), could be used for the purposes of 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 and letter on February 17, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner