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	Mennonite Economic Development Associates of Canada o/a MEDA (Organization)
Decision number (file number)	P2021-ND-134 (File #016513)
Date notice received by OIPC	July 23, 2020
Date Organization last provided information	July 23, 2020
Date of decision	May 25, 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: • name, • date of birth (less than 1/3 of donors), • address, • telephone number, • email address, • donor history, • relationships and connected records, • constituent codes (describes the donor's involvement), • major donor pledges, • communications/events/appeals that have happened, • custom ratings (used for internal segmentation purposes), • prospect management (cultivation, moves management), • event attendance, and • consent (opt in/out) for different types of communications. 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 Raiser's Edge, a product owned by Blackbaud, to store donor data. • On July 17, 2020, the Organization received confirmation from Blackbaud that it discovered and stopped a ransomware attack in May 2020. A copy of a backup file was stolen and Blackbaud paid a ransom to get it back. The production environment was not compromised. • Blackbaud received assurances that the data was deleted, and assured the Organization that the information has not appeared on the public internet in the intervening time. • Blackbaud informed the Organization that based on the nature of the incident, its research, and third party (including law enforcement) investigation, it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.
Affected individuals	The incident affected 28,861 individuals, including 339 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Performed a PIA and determined the security safeguards in Blackbaud's self-hosted met industry standards. • Implemented multifactor authentication for all users and access to our data is handled through encrypted VPN. • Recommended affected individuals remain vigilant by reviewing account statements and monitoring credit reports and report any suspicious activity or suspected identity theft to the Organization and to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter on July 23, 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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated: *As a best practice, we recommend you remain vigilant by reviewing your account statements and monitoring your credit reports. Promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities.*

	In my view, a reasonable person would consider that contact, identity and donor information could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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, *Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.* 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 a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. The Organization reported the personal information may have been exposed for approximately one (1) month.

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 contact, identity and donor information could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a cybercriminal. The Organization reported that the cybercriminal both accessed and stole the personal information at issue. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make available publicly the personal information at issue. The Organization reported the personal information may have been exposed for approximately one (1) month.

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 the affected individuals by email or letter on July 23, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner