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	ADRA International (Adventist Development & Relief Agency) (Organization)
Decision number (file number)	P2020-ND-190 (File #017471)
Date notice received by OIPC	September 30, 2020
Date Organization last provided information	October 1, 2020
Date of decision	December 16, 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 the individual 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, • address, • telephone number, • date of birth, • giving history, • credit card information, and • bank account information. 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	• In July 2020, the Organization received notice from its third party service provider, Blackbaud, that Blackbaud had discovered a cyberattack on one of its systems that houses donor information. • The Organization reported that the breach was "discovered in May 2020" and "...may have included personal data for some of our ... supporters". • The Organization reported that "A detailed explanation of the incident is available on Blackbaud's website at: blackbaud.com/securityincident." This website describes a ransomware attack, by which cybercriminals were able to remove data from Blackbaud's systems.
Affected individuals	The incident affected 1,737 individuals, including 1 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported Blackbaud "...has put in place dark web monitoring intended to detect trafficking of any of the copied data". The Organization reported that it has reviewed its internal policies on data security and made adjustments.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 24, 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.	In its report of the incident, the Organization did not specifically identify any harm(s) that might result to affected individuals. In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of 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.	The Organization reported: *According to Blackbaud, based on the nature of the incident, their research, and third party (including law enforcement) investigation, they "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."* *Blackbaud believes the risk to individuals whose data was accessed is very low. However, in an abundance of caution,*

	Blackbaud has put in place dark web monitoring intended to detect trafficking of any of the copied data. 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 action, theft of data, ransom demand). Although Blackbaud told the Organization 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 significant harms of identity theft and fraud. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate action, theft of data, ransom demand). Although Blackbaud told the Organization 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 individual 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 in a letter dated September 24, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner