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	Operation Eyesight Universal (Organization)
Decision number (file number)	P2021-ND-319 (File #021647)
Date notice received by OIPC	June 14, 2021
Date Organization last provided information	June 14, 2021
Date of decision	March 7, 2022
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 US-based institution 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: <u>Category #1</u> Supporters (5,344 individuals including 322 deceased) • name, address, marital status, spouse's name, gender, birth place, religion. <u>Category #2</u> Supporters or Donors (32,283 individuals including 1,649 deceased) • name, address, donation history, marital status, spouse's name, gender, birth place, religion, ethnicity. <u>Category #3</u> Volunteers (10 individuals) • name, address, and medical condition. <u>Category #4</u> Donors (36 individuals including 1 deceased individual) • name, address, email, donation history, marital status, spouse's name, gender, birth place, religion.

	<u>Category #5</u> Donors (1,741 individuals including 118 deceased individuals) • name, address, email, date of birth and banking information or credit card (last four digits), donation history, marital status, spouses name, gender, birth place, ethnicity, religion. <u>Category #6</u> Supporters (79 individuals) • name, address, telephone number and email. 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	• On October 15, 2020, the Organization's former third-party service provider, Blackbaud, advised that it had been subject to a ransomware attack in May 2020. As part of that incident, data was exfiltrated from Blackbaud's systems. • The Organization had previously engaged with Blackbaud as a service provider to process donations and store and manage donor, volunteer and supporter information, but had changed suppliers prior to this incident. Unfortunately, Blackbaud did not delete the Organization's information and so it was affected in the incident. • Blackbaud advised that the data that had been exfiltrated from its systems included a file containing the back-up to the Organization's donor database. • Blackbaud investigated and also said that it received confirmation from the perpetrators that the data that was removed was destroyed. • Investigations by law enforcement and external IT forensics experts retained by Blackbaud have found no evidence that data has been shared, misused or made public.
Affected individuals	The incident affected 109,539 Canadian individuals, of which 39,483 individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Directly notified stakeholders or supporters. • Established ongoing communication with Blackbaud and independent professionals to fully understand the situation as it relates to the Organization and its supporters. • Reported the incident to the appropriate regulatory authorities and will continue to work closely with their offices. Blackbaud

	also reported the incident to law enforcement and privacy regulators. • Further strengthening data security measures and will continuously look to make improvements.
Steps taken to notify individuals of the incident	Affected individuals in categories #3 to #6 were notified by letter mail on June 10, 2021 or by email on June 14, 2021 with the exception of deceased individuals. For those individuals with no method of contact a notice was posted on the website operationeyesight.com on June 14, 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: *For category #1, it is [the Organization's] assessment that since the personal information involved in the Incident includes contact information but no email and given the low sensitivity information, there is little risk of serious harm such as fraud or identity theft or of a phishing attack.* *For category #2, it is [the Organization's] assessment that since the personal information involved in the Incident includes contact information but no email and given the low sensitivity information, there is little risk of serious harm such as fraud or identity theft or of a phishing attack.* *For category # 3, it is [the Organization's] assessment that since the personal information involved in the Incident includes medical condition (which was provided by the volunteer for medical emergency purposes) which is sensitive, there is a risk of embarrassment for the individual.* *For category # 4, it is [the Organization's] assessment that since the personal information involved in the Incident includes donation history and contact information, there is little risk of fraud or identity theft, but rather the primary risk to affected individuals is that of a potential phishing attack.* *For category # 5, it is [the Organization's] assessment that since the personal information involved in the Incident includes donation history, contact information, and either all date of birth, banking information or the last four credit card number digits, there are potential risks of identity theft, fraud and financial loss and phishing. Blackbaud has advised that the financial information was encrypted, thereby reducing the risk of identity theft, fraud and financial loss.*

	For category # 6, it is [the Organization's] assessment that since the personal information involved in the Incident includes name and contact information including email address, there is a risk of a potential phishing attack. In my view, a reasonable person would consider that the contact, donor and identity information at issue could be used to cause the harms of identity theft and fraud. It is unlikely encrypted financial information (banking) could be used to cause significant harm. Medical information could be used to cause the harms of hurt, embarrassment and humiliation. Email addresses could be used for phishing purposes, increasing 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 that it … *… is of the view that there is not a real risk of significant harm for categories #1 and #2. The likelihood of significant harm is remote given the low sensitivity of the data, the lack of email address and the likelihood of misuse described below.* *For category #3, composed of volunteers that provided medical information, [the Organization] is of the view that the likelihood that significant harm could result is low. While medical information is sensitive and while it may be embarrassing to have this type of information disclosed to anyone, even to a third party that does not know the individual, the likelihood that significant harm could result is low because of the likelihood of misuse described below.* *[The Organization] is of the view that the likelihood that significant harm could result is low for categories #4 to #6. While Blackbaud has advised (with the assistance of its forensic IT expert) that data was exfiltrated from its environment, based on its interactions with the threat actor and in consultations with its forensic IT expert and law enforcement, it has concluded that the chance of any of the exfiltrated data actually being misused is low.* *The fact that the Incident was caused as a result of the actions of an unknown actor with malicious intent additionally does increase the likelihood that harm could result. However, Blackbaud has advised that banking and credit card information were encrypted, thereby reducing the likelihood that significant harm could result. In addition, the personal information is stored in an unusual file format that requires specific software and a paid licence to interpret.*

	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 intrusion and ransom demand). The perpetrator(s) both accessed and stole the personal information of donors. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.

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, donor and identity information at issue could be used to cause the harms of identity theft and fraud. It is unlikely encrypted financial information (banking) could be used to cause significant harm. Medical information could be used to cause the harms of hurt, embarrassment and humiliation. Email addresses could be used for phishing purposes, increasing 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 malicious intent (deliberate, unauthorized intrusion and ransom demand). The perpetrator(s) both accessed and stole the personal information of donors. The Organization cannot be confident the information will not be misused, further disseminated or otherwise made available publicly.

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).

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…", although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Where the information at issue was that of deceased persons, the Organization reported that notification would not be possible because there was, "… no method of contact." For those individuals, the Organization posted a notice on the website operationeyesight.com on June 14, 2021.

I accept that direct notice is not reasonable where the Organization does not have contact information.

I understand the Organization notified the affected individuals in categories #3 to #6 by letter mail on June 10, 2021 or by email on June 14, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner