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	Food Banks Canada (Organization)
Decision number (file number)	P2020-ND-197 (File #016634)
Date notice received by OIPC	August 7, 2020
Date Organization last provided information	September 21, 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 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"	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. "Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*." In this case, the Organization is incorporated under the *Canada Not-for-profit Corporations Act* and does not qualify as a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. Therefore, PIPA applies in this case.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • individual name, • email address, • mailing address, • telephone number, • date and amount of donation,

	• method of payment, • card type used to make the donation. 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 July 16, 2020, the Organization was notified by its third-party fundraising software provider, Blackbaud, that Blackbaud had experienced a ransomware attack. • The cybercriminal was prevented from blocking Blackbaud's system access and fully encrypting files; however, prior to locking the cybercriminal out, a copy of a backup file was removed from the Blackbaud system. The breach occurred between February 7, 2020 and May 20, 2020. • Blackbaud paid the ransom demand after receiving confirmation that the copy of the backup file had been destroyed by the cybercriminal. Blackbaud advised that 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. • Blackbaud retained outside experts to monitor the web and have found no evidence that any information has been released.
Affected individuals	The incident affected 38,529 individual donors of which 2,135 were Albertans; and of the 25,263 other individuals, 1,722 were Albertans.
Steps taken to reduce risk of harm to individuals	The Service Provider: • Confirmed it was able to identify and fix the vulnerability. • Confirmed through testing by multiple third parties that its fix withstands all known attack tactics. • Enhancing access management, network segmentation, deployment of additional endpoint and network-based platforms. The Organization: • Notified affected individuals and data protection regulators. • Posted a notification on its website to notify any individuals for whom it does not have valid contact information.

Steps taken to notify individuals of the incident	Affected individuals for whom the Organization had contact information were notified of the incident by August 7, 2020. A public notice was published on the Organization's website to notify any individual for whom the Organization does not have valid contact information.
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 it "… considers the affected personal information to present a low risk of harm. The information is not sensitive identity information likely to result in identity theft or related harms and no financial information able to be used for fraud was compromised. The only potential risk is of phishing". In my view, a reasonable person would consider that, particularly when combined with profile information (i.e. that individuals are donors of the Organization), individual names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' 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 did not specifically provide an assessment of the likelihood that significant harm would result from 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 said its service provider reported 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. However, the Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors and other individuals. The personal information was in the cybercriminal's possession for approximately three months.
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, particularly when combined with profile information (i.e. that individuals are donors of the Organization), individual names, mobile telephone numbers and email addresses could be used for the purposes of phishing or smishing, increasing the affected individuals' 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 a deliberate unauthorized intrusion by a cybercriminal. The Organization said its service provider reported 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. However, the Organization reported that the cybercriminal had already both accessed and stolen the personal information of donors and other individuals. The personal information was in the cybercriminal's possession for approximately three months.

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."

In this case, the Organization reported that it provided direct notification by August 7, 2020 to those individuals for whom it had valid contact information. However, the Organization it did not have valid contact information for some individuals and therefore posted a notification on its website homepage (https://www.foodbankscanada.ca/Notice-of-Blackbaud-Data-Breach.aspx) for 30 days. The Organization also established a dedicated call centre for individuals seeking additional information regarding the incident.

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner