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	Edmonton Meals on Wheels (Organization)
Decision number (file number)	P2022-ND-023 (File# 021422)
Date notice received by OIPC	June 8, 2021
Date Organization last provided information	June 8, 2021
Date of decision	April 25, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization reported that it is incorporated under Alberta's *Societies Act* and therefore is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. 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. In this case, the Organization operates a meal delivery service at a cost. In my view, the Organization is engaging in commercial activities. To the extent the personal information at issue in this matter was collected, used and disclosed by the Organization in connection with these activities, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information: • name, • home address, • e-mail address, • telephone number, • date of birth, • place of birth,

	• gender, • marital status, • delivery instructions (for certain clients), • bank account number, • driver's license information, and • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 7, 2021, the Organization discovered that an external backup drive was missing from the server room of its head office in Edmonton, AB. • The drive was one of several used to record daily backups of the Organization's primary data server. • The data server from which the backup drive was taken is located in a server room, which requires a keycode to access. • The Organization discovered the encryption function on the scheduled daily backups of the server was disabled sometime prior to the incident. • The Organization reported much of the information contained on the missing backup drive requires the use of third party software to be readable. However, as the data is not in an encrypted format, the Organization has assumed that all of the data on the missing drive has been compromised.
Affected individuals	The incident affected 27, 163 individuals.
Steps taken to reduce risk of harm to individuals	• The Organization reported the incident to the police, but to date, no perpetrator has been identified. • Offered one year of credit monitoring and identity theft protection services at no cost. • Formed a sub-committee to review the adequacy of its technology and security practices. • Enabled the encryption function on all backup processes. • Changed the passcode to the server room. • Reviewed and reinforced its policies and procedures regarding privacy and the collection, use, storage, and retention of personal information. • Retaining a new IT vendor. • Intends to migrate as many of its operational activities and data storage needs to a secure cloud environment.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter, email and telephone on June 7, 2021 and 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, *Depending on the type of personal information pertaining to them, affected individuals are potentially exposed to harms including phishing, fraud, and identity theft as a result of this incident.* In my view, a reasonable person would consider that the contact information at issue, along with the fact the individuals receive services at their home, could be used to cause the harms of humiliation, and distress, and to target the individuals for other harms, such as theft. The contact, identity and financial information could be used to cause the 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, *EMOW has no knowledge or reason to believe that the intent of this incident was to harvest the personal information contained on the backup drive. Furthermore, EMOW is not aware of any of the personal information contained on the backup drive having been misused, as of the date of this report. However, the data on the backup drive is in an unencrypted format and the drive appears to have been taken by a malicious actor rather than simply misplaced. In totality, EMOW considers the affected individuals to be at a real risk of harm and have taken the necessary steps to notify all affected individuals.* In my view, a reasonable person would consider that the likelihood of significant harm is increased because the incident appears to be caused by malicious intent. The risk of harm is increased as the information has not been recovered. In particular, the affected individuals are members of a vulnerable population who receive services from the Organization at their home address. Although the Organization reported that it "has no knowledge or reason to believe that the intent of this incident was to harvest the personal information contained on the backup drive", I do not find this to be reassuring. The Organization can only speculate as to the motives of the person who removed the drive. Lastly, I do not

	believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

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.

In my view, a reasonable person would consider that the contact information at issue, along with the fact the individuals receive services at their home, could be used to cause the harms of humiliation, and distress, and to target the individuals for other harms, such as theft. The contact, identity and financial information could be used to cause the 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 is increased because the incident appears to be caused by malicious intent. The risk of harm is increased as the information has not been recovered. In particular, the affected individuals are members of a vulnerable population who receive services from the Organization at their home address.

Although the Organization reported that it "has no knowledge or reason to believe that the intent of this incident was to harvest the personal information contained on the backup drive", I do not find this to be reassuring. The Organization can only speculate as to the motives of the person who removed the drive. Lastly, I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that affected individuals were notified by letter, email and telephone on June 7, 2021 and June 14, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner