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	CARE Canada (Organization)
Decision number (file number)	P2022-ND-070 (File #024866)
Date notice received by OIPC	February 28, 2021
Date Organization last provided information	May 5, 2022
Date of decision	January 9, 2023
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 not-for-profit organization in the field of relief, reconstruction and development in developing countries. 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 federally incorporated under the *Canada Not-for-profit Corporations Act*. Therefore, it 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. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.

Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information: • name, • address (street, city, province, postal code), • email address, • telephone number, • donation information (donation amount, donation date), • date of birth, • credit card information (credit card type, card number, expiry date), • bank account information (branch transit number, routing number), and • login/password information (for current/former staff). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website and/or application.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In October 2021, the Organization was the victim of a Microsoft Office365 tenant compromise, which is shared between CARE Canada and sister organizations CARE International United Kingdom ("CARE UK") and CARE United States ("CARE USA"). • Three compromised CARE UK service accounts, with Office 365 Administrator Privileges, were compromised and accessed CARE UK's application. • This resulted in the unauthorized access of 3,845 unique pages, emails, and files, from across the shared Office 365 environment, many of which belonged to the Organization and contained personal and/or sensitive information. • On November 8, 2021, the Organization was notified of the incident and began to investigate. • Between January 7, 2022 to February 9, 2022, the Organization became aware of its responsibilities under Alberta PIPA. • In February, 2022, the Organization conducted an assessment of the real risk of significant harm to individuals.
Affected individuals	The incident affected approximately 25,000 individuals including approximately 6,700 individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	The Organization reported several steps taken to reduce risk of harm to individuals including, but not limited to: • Engaged a range of resources to assist in the investigation of the incident. • Suspended and performed remediation and password resets for all known-compromised accounts. • Enforcing multi-factor authentication. • Providing follow-up password hygiene for all CARE Canada users. • Patching vulnerabilities on servers. • Training CARE Canada employees, volunteers, contractors. • Reviewing and hardening user access controls.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, telephone and mail between March 30, 2022 and April 20, 2022.
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, *A breach of an individual's name, address, date of birth, bank account information, and/or credit card number could result in identity theft, financial fraud, and/or negative effects on credit record.* *A breach of an individual's name, email address, telephone number, and/or donation information could result in email phishing, spear-phishing, and/or SMS-phishing attacks.* *A breach of an individual's name, email address, telephone number, and/or donation information could result in identity theft, financial fraud, and financial loss.* *A breach of a CARE Canada employee's login/password could be used to compromise other online accounts.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, and financial information at issue could be used to cause the harms of identity theft, fraud, negative effects on credit record and financial loss. Confirmed valid credentials could be used to compromise online accounts. 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 Organization reported,

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.	*There is a likelihood that harm could result.* *Contact information, including email addresses and telephone numbers, in association with the individual's relationship to the Organization, could be used for phishing purposes and phone scams, increasing vulnerability to identity theft and fraud.* *Affected individuals might include vulnerable individuals, such as youth and seniors.* *The risk of harm is increased as the incident was a result of a deliberate attack on CARE UK's ManageEngine environment, which resulted in the unauthorized access of files belonging to CARE Canada and that contained personal and/or sensitive information.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious actions (unauthorized access). The Organization reported that credentials were used to access accounts illegally and without authorization. Further, the information may have been exposed for approximately three (3) weeks.

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.

The contact, identity, and financial information at issue could be used to cause the harms of identity theft, fraud, negative effects on credit record and financial loss. Confirmed valid credentials could be used to compromise online accounts. 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 harm resulting from this incident is increased because the incident appears to be the result of malicious actions (unauthorized access). The Organization reported that credentials were used to access accounts illegally and without authorization. Further, the information may have been exposed for approximately three (3) weeks.

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 affected individuals by email, telephone and mail between March 30, 2022 and April 20, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance