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	The Canadian Red Cross Society (Organization)
Decision number (file number)	P2022-ND-083 (File #024728)
Date notice received by OIPC	March 7, 2022
Date Organization last provided information	May 20, 2022
Date of decision	January 10, 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 the 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 part of the humanitarian Restoring Family Links Network ("RFL") of the International Red Cross and Red Crescent Movement ("Movement"). The Organization operates on a not-for-profit basis. "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.* 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 because 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 *"Restoring Family Links ("RFL") case records may contain the personal information of an enquirer, a missing/separated person ("Sought Person"), an unaccompanied family member, an individual who is or has been detained outside of Canada ("Detainee") and the recipient of their messages, and/or any individual appointed to speak on behalf of an enquirer, including:"*

	• each individual's full name and/or contact details (including last known address, mailing address, email address and/or phone number), • unique file number assigned to an individual by the National Society/the International Committee of Red Cross ("ICRC"), • any personal information contained in the narrative provided to the Organization about the circumstances related to the enquirer's or beneficiary's request, • copies of a Sought Person's or Detainee's identification, passport and/or photograph, • a Sought Person's or Detainee's date of birth, • the dates, locations and circumstances of a Detainee's arrest/capture, detention, visit by the ICRC, release, repatriation and/or death, • a Detainee's nationality and mother's maiden name, • any personal family message/information contained in any communications between a Detainee and their family that are facilitated by the Organization and/or ICRC, and/or • any personal health information contained within a Sought Person's or separated child's file, for example if the person was last seen at a hospital or has a disclosed disability. 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	• To participate in the RFL program and provide this assistance, the Organization collects and inputs personal information into the international RFL system. This system is managed by ICRC and stored by ICRC's external data centre service providers. • On January 19, 2022, the Organization was advised by ICRC that the RFL system was the subject of a cyber security incident starting on November 2, 2021. • ICRC indicated to the Organization that it has no immediate indications as to who carried out this attack, if the perpetrator had any particular intention, or the technical methodology used by the attacker. • ICRC also confirmed to the Organization that, while there is evidence that information on the RFL system was accessed, this was not a ransomware attack.

	• Based on its investigation thus far, ICRC believes that, information contained in the RFL system has not been tampered with, lost, deleted, published or traded.
Affected individuals	The incident affected approximately 297 individuals, including 7 with a connection to Alberta. The Organization reported, *"Given the nature of some of the services offered through the CRC's RFL program, we are not able to conclude with certainty how many potentially affected individuals have a connection to Alberta. For example, there are some records which include tracing requests for sought individuals who are believed to be in Alberta, however we do not have confirmation that these sought persons are indeed located in Alberta."*
Steps taken to reduce risk of harm to individuals	The ICRC has taken steps to reduce risk of harm to individuals, including: • Working closely with the Movement's worldwide RFL network to understand the scope of the incident. • Reported the incident to law enforcement in Switzerland. • Suspended all access to the compromised systems. Took the compromised servers offline to reduce the immediate impact of the incident. • Hired an independent audit firm to confirm the integrity of the affected information. • The Organization will continue to enhance its data protection capabilities and standards. The Organization has taken steps to reduce risk to individuals, including: • Undertaking an independent review of local systems and services to ensure that they remain secure. • Instructed staff to change login credentials. • Working to assess the impact this incident has had on the individuals it supports. • Continue to evaluate its practices vis-a-vis the RFL program to confirm whether there are further appropriate protective measures that could be implemented to protect personal information.
Steps taken to notify individuals of the incident	The Organization directly notified seven (7) individuals with a connection to Alberta. The Organization has also provided direct notification to all potentially affected Organization personnel who are located in Alberta.

	The Organization reported, *"Given the nature of the Organization's services and the personal circumstances of the individuals we assist, such as missing or displaced persons and detainees, providing direct notification to other potentially affected individuals is highly impractical, if not impossible. Attempting to provide direct notification to detainees may also create security concerns, as messages to detainees are generally subject to screening by the detaining organization. Accordingly... the Organization has provided indirect notification by way of statement on the Restoring Family Links website, which remains posted today."*
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, *"Individuals whose contact and/or identification information was impacted may be at risk of phishing, identity theft or other fraudulent activities. Depending on the nature of the individuals' circumstances, they may be at risk of harms such as embarrassment, hurt and/or damage to relationships."* I agree with the Organization's assessment. The contact and identity information could be used to cause the harms of identity theft and fraudulent activities. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Health information and information about an individual's circumstances could be used to cause the significant harms of hurt, humiliation, hurt, embarrassment and/or damage to relationships. 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, *The intent of the attacker is still unknown. At this stage, the ICRC has indicated to us that there is no evidence of the attacker tampering with or deleting personal information stored in the RFL database.* *The ICRC has further advised us that there is not yet any indication that the information stored in the RFL database has been leaked or shared publicly. It is possible that the information could be unlawfully used or disclosed in the future.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The information may have been compromised for approximately two (2) months. The fact that "*there is not yet any*

	indication that the information stored in the RFL database has been leaked or shared publicly..." does not mitigate against the possibility of future use of the information to cause the significant harms identified previously.

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.

Contact and identity information could be used to cause the harms of identity theft and fraudulent activities. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Health information and information about an individual's circumstances could be used to cause the significant harms of hurt, humiliation, hurt, embarrassment and/or damage to relationships. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The information may have been compromised for approximately two (2) months. The fact that "there is not yet any indication that the information stored in the RFL database has been leaked or shared publicly..." does not mitigate against the possibility of future use of the information to cause the significant harms identified previously.

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 the seven affected individuals with a connection to Alberta and all potentially affected Organization personnel who are located in Alberta in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

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."

Given the Organization's submissions, I accept that indirect notice as described by the Organization is reasonable for those affected individuals whose personal information was collected in Alberta who were not able to be notified directly.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance