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	Juvenile Diabetes Research Foundation (Organization)
Decision number (file number)	P2018-ND-002 (File #006778)
Date notice received by OIPC	October 10, 2017
Date Organization last provided information	October 10, 2017
Date of decision	January 2, 2018
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 is a national charitable organization that conducts operations in Alberta and other Canadian jurisdictions and has Alberta-based employees. The Organization operates on a not-for-profit basis. 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, the Organization is fully subject to PIPA.

Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information about the individuals, who are employees or former employees of the Organization: • name, • date of birth, • home address, • emergency contact information, • telephone number, • Social Insurance Number, and • salary. 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	
	• On August 1, 2017, and again on August 17, 2017, an intruder accessed the Organization's human resources data base using misappropriated administrator credentials. The accesses lasted for 1 and 35 minutes each, respectively. • The database contains approximately 300 records of current and former employees. • A human resources employee discovered the unauthorized accesses on August 21, 2017. • The Organization's access logs indicate the intruder made several changes to the database information, including to vacation requests, user profiles, salary and address information. • The Organization reported that its HR database provider "believes that the person responsible obtained the Admin username and password either as a former employee or from a former employee."
Affected individuals	The affected individuals included 3 Alberta employees.
Steps taken to reduce risk of harm to individuals	• Offered one year of free identity theft and credit monitoring services to the affected individuals. • Restored all human resources information to its original condition. • Reported the incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on September 29, 2017.

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 "This incident raises the possibility of fraud, identity theft, and negative effects on credit records." I agree with the Organization. The identity and employment information could be used to cause the harms of 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 reported that it believes the likelihood of harm to the three Alberta employees is low because "There is no evidence that any information was downloaded, or of any other exfiltration, according to the security logs" and "The user profiles of 3 of the Alberta employees were accessed for between approximately 10 and 30 seconds each". In my view, the likelihood of harm resulting from this incident is increased because the intruder not only accessed the personal information, but made changes, indicating deliberate and possibly malicious intent. Further, the second intrusion lasted 35 minutes, which is ample time to copy the information. The Organization advised that there was no evidence to suggest the intruder retained the information, but did not present evidence to show the information was not exfiltrated.

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 identity and employment information could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the intruder not only accessed the personal information, but made changes, indicating deliberate and possibly malicious intent. Further, the second intrusion lasted 35 minutes, which is ample time to copy the information. The Organization advised that there was no evidence to suggest the intruder retained the information, but did not present evidence to show the information was not exfiltrated.

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

I understand the Organization notified the affected individuals in a letter dated September 29, 2017, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner