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	Desjardins Financial Security (the Organization)
Decision number (file number)	P2021-ND-057 (File #013123)
Date notice received by OIPC	September 6, 2019
Date Organization last provided information	January 7, 2020
Date of decision	March 9, 2021
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 individual whose 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 the life and health insurance arm of Desjardins Group, a financial institution in Quebec. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • group number, • participant number, and • date of birth. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Between June 25, 2019 and July 31, 2019, an employee of the Organization accessed and used personal information of a number of group retirement savings participants (only one resides in Alberta) for fraudulent transactions.

	• The breach was discovered on July 29, 2019, when an irregular online transaction was blocked and reported. The Organization investigated, which led to the employee in question.
Affected individuals	The incident affected 36 individuals, including one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Blocked online transactions for affected individuals and transactions were reimbursed. • Suspended employee who was interrogated by local police.
Steps taken to notify individuals of the incident	The affected individual was notified of the incident by letter on January 7, 2020.
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 the possible harms that may occur as a result of the breach are "Fraud, identity theft, financial loss, and stress." I agree with the Organization's assessment. A reasonable person would consider the identity information at issue could be used to cause the harms of fraud, identity theft, and financial loss in particular. 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.	With respect to the likelihood of harm resulting from this incident, the Organization reported, *It already happened, though every amount was reimbursed. The risk of future harm will be assessed with the investigation although the possibility of on line transaction is thoroughly monitored in other groups and blocked for affected individuals.* 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 employee (deliberate intrusion) and the information was exposed for over one (1) month. The Organization reported that harm has already occurred.
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 resulting from this incident. A reasonable person would consider the identity information at issue could be used to cause the harms of fraud, identity theft, and financial loss in particular. These are 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 employee (deliberate intrusion) and the information was exposed for over one (1) month. The Organization reported that harm has already occurred.

I require the Organization to notify the affected individual 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 affected individual by letter on January 7, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner