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 Group (Organization)
Decision number (file number)	P2021-ND-056 (File #013445)
Date notice received by OIPC	June 20, 2019
Date Organization last provided information	December 10, 2019 (The Organization provided an updated submission that was originally assigned OIPC File #14127)
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 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 Canadian financial services cooperative, based in Montreal, 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: • first and last name, • date of birth, • social insurance number, • address, • telephone number, • email address, and • details about banking habits and products. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization also reported that, of the affected parties in Alberta, "seven were individuals and seven were corporate contacts (i.e. representatives of businesses)." As such, some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to

	mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to this information.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 14, 2019, the Organization learned from police that one of its employees exfiltrated client personal information over the course of at least 26 months. • Police found files containing the personal information of 9.7 million active and inactive files of individuals during a police search in a fraud and identity theft case. • As part of the employee's responsibilities, the employee had access to personal information of banking members as well as credit cardholders and clients with in-store financing.
Affected individuals	The incident affected approximately 9.7 Million individuals, including 3,350 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Fired the employee. • Worked with local police. • Implemented security measures on all accounts of affected individuals. • Improved procedures for confirming members' identity in person and over the phone. • Will provide identity theft protection to all members and clients who do business with the Organization. • Encouraged to adopt good habits to ensure their assets, transactions and personal information remain secure.
Steps taken to notify individuals of the incident	Affected individuals were notified indirectly by press conference on June 20, 2019 and directly by letter of June 30, 2019.

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 include "Identity theft, fraud, financial loss, stress. In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing 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 the likelihood that the harm will result is "High because the ex-employee was clearly acting with ill intent." In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee, acting over the course of at least 26 months.

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.

A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee, acting over the course of at least 26 months.

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 that affected individuals were notified indirectly by press conference on June 20, 2019 and directly by letter of June 30, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner