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 Life Assurance Company
Decision number (file number)	P2014-ND-11 (File #P2643)
Date notice received by OIPC	April 2, 2014
Date Organization last provided information	August 22, 2014
Date of decision	September 30, 2014
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 federally incorporated and licenced under the *Alberta Insurance Act* to carry on business in Alberta The information involved was collected in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) [or other applicable subsection] of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information about the individuals: • client names, • financial (mutual funds) information, • medical information (in advisor's notes). This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• A break-in occurred at the Organization's office in Surrey,

	British Columbia on the weekend of March 23, 2014. • 100 paper files containing personal, financial and medical information were stolen. • Two Organization laptop computers were also stolen. The laptops contained insurance illustrations and advisors' notes about client. The laptops were encrypted as was as protected with strong passwords. • On August 21, 2014, the Organization notified the OIPC that the RCMP recovered the missing files. • The RCMP is expected to return the files to the Organization upon concluding its investigation.
Affected individuals	• Two individuals from Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization advised affected individuals, via telephone, to monitor their financial accounts between March 24, 2014 and March 28, 2014. • Affected individuals were also advised to contact Equifax Canada Inc. and TransUnion Canada Inc. and request for credit record monitoring. • The two stolen laptops were encrypted and protected with strong passwords.
Steps taken to notify individuals of the incident	• The Organization notified affected individuals via telephone on between March 24, 2014 and March 28, 2014. • Formal letters of notification were sent to all affected individuals by April 3, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized the affected individuals may be at risk of harm. In my view, the personal, financial and medical information involved is highly sensitive. The types of harm that could result from unauthorized access or use of the information in this instance are identity theft, financial loss and/or fraud, and hurt and/or humiliation.
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	The Organization reported that it believes there is a real risk of significant harm that could result from this incident. In my view, the likelihood of harm resulting from this incident is increased because the unauthorized access resulted from malicious intent (a break-in). Although the paper files were eventually recovered they were exposed for a period of

incident and the possible harm.	approximately 5 months. There is no real risk of significant harm resulting from unauthorized access to the personal information stored on the stolen laptops, given that the laptops were protected by encryption in addition sot strong passwords.

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 personal information involved sensitive personal, financial and medical information and was accessed by an unauthorized individual with malicious intent. Although the paper files were eventually recovered they were exposed for a period of approximately 5 months. There is no real risk of significant harm resulting from unauthorized access to the personal information stored on the stolen laptops, given that the laptops were protected by encryption in addition sot strong passwords.

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

I understand the Organization notified the affected individuals, in accordance with the Regulation. The Organization is, therefore, not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner