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	Federated Insurance Company of Canada (Organization)
Decision number (file number)	P2016-ND-11 (File # 000835)
Date notice received by OIPC	May 15, 2015
Date Organization last provided information	May 15, 2015
Date of decision	March 16, 2016
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 incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • date of birth, • Social Insurance Number (SIN), • bank account number, • driver's license information, • background check information, • driving abstracts, • tax information, • performance review information, • salary review information, • emergency contact information, • family pictures, and • personal financial records.

	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	• The Calgary office of the Organization was broken into on May 8, 2015. • The alarm code to the facility was disabled and a stolen key fob was used to facilitate the break-in. • Thieves stole personnel files, two business customer files, and three laptop computers. • The personnel and customer files were in paper form. • The three laptop computers were protected by full disk encryption. • The incident was discovered on May 11, 2015.
Affected individuals	Affected individuals included 32 clients and 28 employees of the Organization.
Steps taken to reduce risk of harm to individuals	• Alarm codes and physical locks were changed. • Security protocols for the cleaning company and other third party service providers were reviewed. • The laptops were removed from the Organization's active directory services (domain) and remote access to the network using the stolen computer was disabled. • Account passwords for the stolen computers were changed. • Affected individuals were provided with credit monitoring.
Steps taken to notify individuals of the incident	Affected employees and client organizations were notified on May 11, 2015.
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 information in the personnel and customer files is highly sensitive and could be used to cause the harms of identity theft, financial loss or fraud. Information in driving records could also cause damage to reputation. I agree with the Organization. The personal information includes sensitive identity and financial information. This information could be used to cause the harms of identity theft, financial loss, fraud, hurt or humiliation and embarrassment. These are significant harms.

	Personal information stored on the encrypted laptops is not accessible and cannot be used to cause significant harm.
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 the stolen files and laptops have not been recovered, nor have the perpetrators been identified or apprehended. Given this, and considering "that the breach is the result of a criminal act", there is a "plausible likelihood" that harm could result from this incident. I agree with the Organization's assessment. In my view, the likelihood of harm resulting from this incident is increased because the personal information was stolen and has not been recovered. In contrast, there is negligible risk associated with any information stored on the stolen laptops because they were encrypted.

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 includes sensitive identity and financial information. This information could be used to cause the significant harms of identity theft, financial loss, fraud, hurt or humiliation and embarrassment. The personal information was stolen and has not been recovered.

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 on May 11, 2015 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner