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	The Statesman Group of Companies Ltd. (Organization)
Decision number (file number)	P2017-ND-52 (File #001506)
Date notice received by OIPC	September 11, 2015
Date Organization last provided information	March 22, 2017
Date of decision	May 15, 2017
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 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: • first and last name, • mailing, • email address, • amount of compensation, • RRSP contribution amount, • credit card information (no security code), • personal income tax submissions (annual earnings, and social insurance number), and • basic medical information. 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	

Description of incident	• On September 6, 2015, an employee's vehicle was broken into and a hard drive containing a copy of the Organization's server was stolen. • The theft was discovered on September 7, 2015. • The hard drive was locked in the vehicle in a detached garage. • The hard drive has not been recovered. • The hard drive had no technical security.
Affected individuals	Affected individuals include 30 employees, and 15 residents in seniors' communities operated by the Organization.
Steps taken to reduce risk of harm to individuals	• Reported the theft to the Calgary Police Service on September 7, 2015. • Reported the theft to Human Resources and in-house Legal Counsel on September 8, 2015. • Notified affected employees by email on September 8, 2015. • Notified Senior Community Managers who had individual discussions with potentially affected residents. • In the process of switching IT providers and will be backing up all information in a new secure manner.
Steps taken to notify individuals of the incident	• Notified affected employees by email on September 8, 2015. • Notified Senior Community Managers who had individual discussions with potentially affected residents.
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.	In its report of the incident, the Organization reported that potential harms resulting from this incident include "damage to reputation, identity theft, or fraud." I agree with the Organization. The personal information at issue includes identity, financial, employment, and medical information that could be used to cause the harms of identity theft, fraud, financial loss, phishing, damage to reputation, and negative effects on a credit record. 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 "There is a remote potential for harm. While we do not know who obtained the information, and it was obtained without any security measures in place it is most likely that the theif [sic] will wipe the drive for resale. That being said, the information can be viewed as highly sensitive, and has been missing for 3 days. It is possible that the information could be used for criminal purposes as it has not been recovered."

	In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft), indicating malicious intent. The laptop was not encrypted, the information has not been recovered and some of the information concerns a vulnerable population. Although the Organization does not believe the information was the target of the theft and have no knowledge of the information being used or disclosed, it is impossible to know this for sure.

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 at issue includes identity, financial, employment, and medical information that could be used to cause the harms of identity theft, fraud, financial loss, phishing, damage to reputation, and negative effects on a credit record. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft), indicating malicious intent. The laptop was not encrypted, the information has not been recovered and some of the information concerns a vulnerable population. Although the Organization does not believe the information was the target of the theft and have no knowledge of the information being used or disclosed, it is impossible to know this for sure.

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 writing and in person on September 8, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner