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	Rail Europe North America Inc. (Organization)
Decision number (file number)	P2018-ND-116 (File #008735)
Date notice received by OIPC	May 22, 2018
Date Organization last provided information	July 5, 2018
Date of decision	August 13, 2018
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 Delaware corporation that conducts business in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • credit card number, • username and password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. For some individuals, the information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• As a result of queries from one of the Organization's banks, the Organization commenced an investigation of its ecommerce websites, which are used by persons outside of the EU to purchase rail passes for use in EU countries. • Specifically, the Organization's parent company, Rail Europe SAS (France), which operates the IT platform to which the Organization migrated its ecommerce websites, engaged two forensic analysis and security auditing firms to investigate. • To date, the investigation has revealed that unauthorized persons gained unauthorized access to the IT platform to which the Organization was migrating its ecommerce websites, beginning in November 2017. • The Organization reports the incident occurred between November 29, 2017 and February 16, 2018. • The incident was discovered on February 16, 2018.
Affected individuals	The Organization said its report was "notification of unauthorized access to the personal information … of 190 residents of Alberta, Canada."
Steps taken to reduce risk of harm to individuals	• Shut down the ecommerce websites when breach was discovered. • Cut-off and isolated all compromised servers from the Internet. • Removed all untrusted components. • Changed passwords on all systems and applications. • Renewed certificates and hardened security controls. • Froze all function changes on the affected websites in order to detect and prevent any new attempt to compromise the systems.
Steps taken to notify individuals of the incident	Affected individuals have not been notified.
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 did not identify the potential harm(s) that may result from this incident. In my view, a reasonable person would consider that the financial information (credit card information) at issue could be used to cause the harms of identity theft, fraud and financial loss. Credentials (user name and password) could be used to compromise other online accounts where individuals may have used the same credentials, potentially causing further harms of identity theft and fraud. 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 did not specifically assess the likelihood of harm resulting from this incident. 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 unknown third party (deliberate intrusion and installation of spyware). Many individuals use the same credentials across various online accounts and those accounts remain vulnerable. The information may have been exposed for over 2 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 financial information (credit card information) at issue could be used to cause the harms of identity theft, fraud and financial loss. Credentials (user name and password) could be used to compromise other online accounts where individuals may have used the same credentials, potentially causing further harms of identity theft and fraud. 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 unknown third party (deliberate intrusion and installation of spyware). Many individuals use the same credentials across various online accounts and those accounts remain vulnerable. The information may have been exposed for over 2 months.

I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to my office in writing, within 10 days of the date of this decision, that it has done so.

Jill Clayton
Information and Privacy Commissioner