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 SAS (France) (Organization)
Decision number (file number)	P2018-ND-117 (File #009033)
Date notice received by OIPC	June 28, 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information for customers who completed purchases, or created or accessed their accounts on the Organization's websites during the period of compromise. • 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. To the extent this information was collected in Alberta via the Organization's website, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In mid-2017, thru PHP code injection, an attacker was able to gain access to Organization's front-end web servers and install spyware in order to collect data entered by customers on the Organization's website.

	• The data encryption in place between the Organization's web browsers and servers did not protect the customer information from the attacker due to the method of attack. • The incident occurred between June 15, 2017 through February 16, 2018. • The incident was discovered on February 16, 2018, as a result of queries from one of the Organization's banks. • The Organization undertook an investigation of its ecommerce websites, which are used to purchase rail passes for use in EU countries, and engaged two forensic analysis and security auditing firms to investigate the possible incident.
Affected individuals	The Organization did not provide an estimate of the number of affected individuals, or the number of individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Shut down the ecommerce websites. • 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 affected websites so as to detect and prevent any new attempt to compromise the systems. • Notified "certain other regulators throughout the months of April and May 2018."
Steps taken to notify individuals of the incident	The Organization reported "Alberta residents 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 reported "There is a low possibility of identify [sic] theft" and "Credit card information may have been compromised, which is considered more sensitive. The other information that may have been compromised (username, name, password) is relatively benign." In my view, a reasonable person would consider that the financial information at issue (credit card information) 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 reported "In our opinion, the breach does not pose a real risk of significant harm to individuals because the credit card brands and banks were quickly notified, and Rail Europe shut down the affected ecommerce websites as soon as the possibility of a breach was discovered." Further, "Harm is not likely to result, because Rail Europe notified credit card brands and the information potentially compromised is now stale." 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). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Many individuals use the same credentials across various online accounts and those accounts remain vulnerable. Further, the information may have been exposed for almost 8 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 at issue (credit card information) 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). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Many individuals use the same credentials across various online accounts and those accounts remain vulnerable. Further, the information may have been exposed for almost 8 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