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	Premiere Suites (Organization)
Decision number (file number)	P2019-ND-169 (File #013353)
Date notice received by OIPC	June 4, 2019
Date Organization last provided information	June 4, 2019
Date of decision	November 22, 2019
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 all or some of the following information: • first and last name, • email address, • telephone number, • employer name, and • credit card information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or around May 30, 2019, one of the Organization's laptop computers was stolen. • Despite company policy to the contrary, credit card information was stored on the hard drive. As a result, the data contained on the hard drive might have been accessible to the public.

	• The incident was reported on May 31, 2019, and the account was frozen early in the morning of Saturday, June 1.
Affected individuals	The Organization did not report the number of affected individuals.
Steps taken to reduce risk of harm to individuals	• The impacted employee's company account was frozen. • Taken steps to re-educate users on the information that can and cannot be stored in the operating system and the procedures to report theft of a personal computer. • Will roll out updated, more secure authentication system for users who require CRM access. All CRM users will be required to use a multi factor authentication login system.
Steps taken to notify individuals of the incident	The Organization reported that it "…has notified all of the impacted parties".
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 specifically identify any potential harms that might result from the incident. In my view, a reasonable person would consider the contact, employment, and financial information at issue could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 the incident. In my view, a reasonable person would consider that 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 (stolen laptop), and the information has not been recovered.
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 the contact, employment, and financial information at issue could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.	

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 (stolen laptop), and the information has not been recovered.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

The Organization reported that it "…has notified all of the impacted parties" but did not provide any details of this notification. **I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that it has notified affected individuals whose personal information was collected in Alberta, in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner