



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Fontainebleau Miami Beach (Organization)
Decision number (file number)	P2019-ND-019 (File #008658)
Date notice received by OIPC	May 9, 2018
Date Organization last provided information	May 9, 2018
Date of decision	February 14, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual whose personal information was collected in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• credit/debit card number and expiry date. <p>This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On January 3, 2018, the Organization learned that certain guests’ credit card information was accessed without authorization.• The Organization investigated and discovered that the credit card information was acquired between November 2017 and January 2018.

Affected individuals	The incident affected one individual in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Launched an investigation. • Contacted law enforcement. • Provided notice to affected individuals. • Provided guidance on how affected individuals can better protect against identity theft and fraud. • Provided notice to other state regulators as required by law.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on May 2, 2018.
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 harm that might result from this incident, but its notification to affected individuals said “We encourage you to remain vigilant against incidents of identity theft and fraud”. In my view, a reasonable person would consider that the contact and financial information at issue (including payment card numbers and expiry dates) could be used to cause the significant harms of 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 provide an assessment of the likelihood that significant harm would result from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for over two 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 individual. A reasonable person would consider that the contact and financial information at issue (including payment card numbers and expiry dates) could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The personal information may have been exposed for over two months. I require the Organization to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).	

I understand the Organization notified the affected individual in a letter dated May 2, 2018 in accordance with the *Regulation*. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner