



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Holloway Lodging Corporation (Organization)
Decision number (file number)	P2018-ND-020 (File #007395)
Date notice received by OIPC	January 3, 2018
Date Organization last provided information	January 3, 2018
Date of decision	January 29, 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 the individuals 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,• telephone number,• rewards number,• email address,• last four digits of credit card used to reserve the room. <p>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, I have jurisdiction in this matter.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• Early on December 11, 2017, a storage area at the Organization’s Super 8 hotel in Fort St. John, BC was broken into.

	<ul style="list-style-type: none"> • Boxes containing records for guests who stayed at the hotel during the months of January, May - August, November and December 2015 were stolen. • The Organization learned of the incident the same day. • An individual has been apprehended by the police in connection with the theft. Some of the records have been recovered and are being held by the police.
Affected individuals	The incident affected approximately 3,000 individuals. The Organization did not provide an estimate of the number of affected residents of Alberta.
Steps taken to reduce risk of harm to individuals	Reported the incident to law enforcement, and the British Columbia and Alberta privacy commissioners.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent January 3, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization did not specifically identify any harm that might result from the incident, but recommended that affected individuals take steps to, among other things, request a credit report and “place a fraud alert on your credit report” to “help prevent an identity thief from opening additional accounts in your name.”</p> <p>In my view, the contact, profile information (rewards number) and email address could be used for phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm.</p>
<p>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.</p>	<p>The Organization did not specifically assess the likelihood of harm resulting from this incident.</p> <p>In my view, the likelihood of harm is increased as the incident resulted from malicious intent (break-in and theft). Although an individual has been apprehended, not all of the information has been recovered and may have been used or further distributed.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
Given the information reported by the Organization, and considering the circumstances in this case, I have decided that there is a real risk of significant harm to the affected individuals.	

The contact, profile information (rewards number) and email address could be used for phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm. The likelihood of harm is increased as the incident resulted from malicious intent (break-in and theft). Although an individual has been apprehended, not all of the information has been recovered and may have been used or further distributed.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by letter sent January 3, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner