



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	The Glencoe Club (Organization)
Decision number (file number)	P2019-ND-092 (File #011954)
Date notice received by OIPC	February 5, 2019
Date Organization last provided information	February 5, 2019
Date of decision	June 27, 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 pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	<p>The Organization reported that it is incorporated under Alberta’s <i>Societies Act</i> and therefore is a “non-profit organization” as defined in section 56(1)(b)(i) of PIPA.</p> <p>Pursuant to section 56(2), PIPA “does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization”, except in the case of personal information that is collected, used or disclosed in connection with any commercial activity.</p> <p>In this case, the Organization operates a private sports club, collects membership fees, and provides programs and services as well as operating food and beverage facilities. In my view, the Organization is engaging in commercial activities. To the extent the personal information at issue in this matter was collected, used and disclosed by the Organization in connection with these activities, PIPA applies.</p>
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• Organization member number,• date of birth,• email address (personal or business - whatever was on file),• home telephone number, and• some personal cell numbers.

	This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.
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"> On January 20, 2019, an employee took home rosters for children's swimming lessons. The rosters were in a binder, the binder was in a bag, and the bag was left in the employee's personal vehicle overnight. At some point over the course of the night the employee (and others) had their vehicle broken into and the bag was removed. The incident was discovered on January 21, 2019. The personal information has not been recovered.
Affected individuals	The incident affected 40 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Reminded supervisors/managers of the appropriate report generating fields to be used to ensure that information of this nature is not produced from the membership software system. Physical verification audits to be completed for departments who provide programs and would produce lists of names.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on January 25, 2019, with a follow-up phone call the same day.
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 the possible harms that might result from this incident include “Identity theft”. I agree with the Organization’s assessment. The contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, leading to increased vulnerability to fraud and identity theft. These are significant harms.

<p>Real Risk</p> <p>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 reported that “The theft appears to be a crime of opportunity to steal valuables that may have been in the work bag. It is not believed that the thieves have any intent to use the information obtained but we are unable to verify this.”</p> <p>In my view, a reasonable person would consider that the risk of significant harm is increased as the breach resulted from malicious intent (vehicle break-in and theft), and the information has not been recovered.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>The contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, leading to increased vulnerability to fraud and identity theft. These are significant harms. A reasonable person would consider that the risk of significant harm is increased as the breach resulted from malicious intent (vehicle break-in and theft), and the information has not been recovered.</p> <p>I require the Organization to notify the affected individuals in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand that affected individuals were notified by email on January 25, 2019, with a follow-up phone call the same day. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner