



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Confederation Park Little League (Organization)
Decision number (file number)	P2019-ND-040 (File #005043)
Date notice received by OIPC	February 24, 2017
Date Organization last provided information	January 9, 2019
Date of decision	March 1, 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 the individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	<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>“Non-profit organization” is defined in section 56(1) to mean an organization “that is incorporated under the <i>Societies Act</i> or the <i>Agricultural Societies Act</i> or that is registered under Part 9 of the <i>Companies Act</i>.”</p> <p>In this case, the Organization is a registered non-profit organization under the <i>Societies Act</i>. According to its website, the Organization charges fees to pay for registration and insurance, uniforms and hats, hoodies and toques, tournament fees, indoor training, extra workshops, and the parent clinic. These are commercial activities.</p> <p>To the extent the information at issue was collected in connection with these commercial activities, PIPA applies.</p>

<p>Section 1(1)(k) of PIPA “personal information”</p>	<p>The information at issue was in a spreadsheet with member contact information and included:</p> <ul style="list-style-type: none"> • first and last name of player (child), • first and last name of child’s parent(s), • personal telephone number, and • email address. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
<p>DESCRIPTION OF INCIDENT</p>	
<p><input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure</p>	
<p>Description of incident</p>	<ul style="list-style-type: none"> ▪ On February 18, 2017, a former volunteer of the Organization sent an email to the Organization’s members informing them of a new baseball program (i.e. a new program that is a competitor to the Organization). ▪ The Organization had allowed volunteers to use their personal email addresses for their volunteer work. The former volunteer had a spreadsheet containing the information at issue, and used this to email the members about the new program. ▪ The former volunteer did not delete or return the information when leaving the Organization. ▪ After the incident, she did not return the personal information to the Organization. ▪ The Organization learned about the incident on February 18, 2017 when members of the Organization contacted the Organization asking why they were receiving the emails and asking who the sender was.
<p>Affected individuals</p>	<p>The Organization reported that its membership included approximately 400 individuals. The Organization did not respond to requests that it confirm the number of affected individuals.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • Reviewed information management practices and contacted the Edmonton Chamber of Volunteers who helped them make changes aligned to best practices. • Revised policies and procedures. • Now requiring all volunteers to sign confidentiality agreements and prohibiting volunteers from using personal emails to email members. • Limiting access to the website/email server that is used to communicate with members.

<p>Steps taken to notify individuals of the incident</p>	<p>The Organization reported that it notified affected individuals about the breach; however, the Organization did not respond to requests for specific details about the notification.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<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 assessed the type(s) of harm that might result from the breach as “A misttust [sic] amongst our members on use of there [sic] personal data and they don’t want to solisted [sic] by a company or indivdual [sic] to go to other programs etc.”</p> <p>In my view, a reasonable person would consider that the personal information at issue could be used to make unsolicited telephone calls, and for phishing purposes, increasing vulnerability to identity theft and fraud. I have previously found phishing, identity theft and fraud to be significant harms.</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 reported “This has created harm to our members trusted there [sic] information is only used for Little League purposes.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate action of a former volunteer, who used it for an unauthorized purpose. The Organization was not able to recover the information, and did not receive confirmation from the former volunteer that the information will not be further used or disclosed. Some of the affected individuals appear to be members of a vulnerable population (children).</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 in this case.</p> <p>A reasonable person would consider that the personal information at issue could be used to make unsolicited telephone calls, and for phishing purposes, increasing vulnerability to identity theft and fraud. I have previously found phishing, identity theft and fraud to be significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate action of a former volunteer, who used it for an unauthorized purpose. The Organization was not able to recover the information, and did not receive confirmation from the former volunteer that the information will not be further used or disclosed. Some of the affected individuals appear to be members of a vulnerable population (children).</p>	

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

I understand the Organization reported that it notified affected individuals about the breach; however, the Organization did not respond to requests for specific details about the notification. **The Organization is required to confirm to my office in writing, within ten (10) days of the date of this decision, that it has notified affected individuals in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner