



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Women's Flat Track Derby Insurance Inc. (Organization)
Decision number (file number)	P2020-ND-082 (File #014503)
Date notice received by OIPC	January 13, 2020
Date Organization last provided information	April 4, 2020
Date of decision	July 24, 2020
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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	<p>The Organization offers insurance coverage to adult and junior flat and banked track leagues operating in North America. Leagues and skaters visiting the U.S. may also purchase insurance from the Organization.</p> <p>The Organization is located in Austin, Texas USA, and is an "organization" as defined in section 1(1)(i) of PIPA.</p>
Section 1(1)(k) of PIPA "personal information"	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• first and last name,• province,• address,• email address,• date of birth,• electronic signature,• provincial health identification,• provincial health card issued,• league name,• type of membership,• payment method,• Canadian Roller Derby Insurance (CDRi) expiration date,• date card was sent,• CRDi region (east or west), and

	<ul style="list-style-type: none"> • other insurance/source of insurance/transaction date/time stamp. <p>This information is about identifiable individuals 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 August 8, 2019, the Organization acquired CRDi and as a result is the owner of the list of, and contact information for, customers with CRDi, past and present, active, cancelled, and pending in an effort to begin developing member solutions for leagues and skaters across Canada. • On December 11, 2019, a former CRDi employee emailed participants to promote a new company. The email was worded in such a way that it confused recipients as to whether the new company was affiliated with the Organization or CRDi. • The former employee had access to email addresses and contact information from CRDi’s database. However, there was no authorization or permission given to use the information by anyone outside the Organization or CRDi.
Affected individuals	The incident affected 2,652 individuals of which 2 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Sent a cease and desist letter to the individuals whom the Organization believes has the unauthorized access to the information. • Sent a follow-up letter. • Sent an invitation letter as part of the investigation to determine the risk of harm and steps to take.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 10, 2020.
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</p>	<p>The Organization did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated:</p> <p style="text-align: center;"><i>Although we are unaware of any use of your information which would create a real risk of significant harm to you, we are providing notice to you and other potentially affected customers about the incident because we are</i></p>

<p>non-trivial consequences or effects.</p>	<p><i>investigating the unauthorized use of information pertaining to your former Canadian Roller Derby, Inc. (CRDi) membership, purchased through crdinfo.ca.</i></p> <p>In my view, a reasonable person would consider that the contact and identity information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are 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 did not specifically assess the likelihood that significant harm would result from this incident.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the Organization does not know if the personal information was compromised due to negligence or malicious intent of the former employee. It is unclear whether the Organization asked the former employee to delete the personal information or confirm that the information has not been further used, copied, disclosed, or otherwise distributed. It appears from the Organization's report that the information was used to contact members.</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>A reasonable person would consider that the contact and identity information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms.</p> <p>The likelihood of harm resulting from this incident is increased because the Organization does not know if the personal information was compromised due to negligence or malicious intent of the former employee. It is unclear whether the Organization asked the former employee to delete the personal information or confirm that the information has not been further used, copied, disclosed, or otherwise distributed. It appears from the Organization's report that the information was used to contact members.</p> <p>I require the Organization to notify the affected individuals 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 individuals in an email dated February 10, 2020 in accordance with the Regulation. The Organization are not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner