



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Women Building Futures Society (Organization)
<b>Decision number (file number)</b>	P2021-ND-233 (File #018995)
<b>Date notice received by OIPC</b>	January 12, 2021
<b>Date Organization last provided information</b>	January 12, 2021
<b>Date of decision</b>	November 22, 2021
<b>Summary of decision</b>	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	<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’s mission is to empower women’s economic prosperity by removing barriers and providing industry recognized training in the construction trades, maintenance, transportation industries and more.</p> <p>In my view, the Organization is engaging in commercial activities.</p> <p>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>

<p><b>Section 1(1)(k) of PIPA “personal information”</b></p>	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none"> <li>• name,</li> <li>• email address,</li> <li>• financial information regarding costs of program,</li> <li>• student support required for living expenses, and</li> <li>• decision to support student with additional funds requested.</li> </ul> <p>This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
--	---

**DESCRIPTION OF INCIDENT**

<input type="checkbox"/> loss	<input type="checkbox"/> unauthorized access	<input checked="" type="checkbox"/> unauthorized disclosure
-------------------------------	--	---

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>• On January 6, 2021, an employee with the Organization sent an email containing a student's financial information to another student in error.</li> <li>• This was the result of typing in an incorrect email address.</li> <li>• The breach was discovered the same day when another recipient of the email, an employee of the Organization, contacted the sender to advise of the error.</li> </ul>
---------------------------------------	--

<p><b>Affected individuals</b></p>	<p>The incident affected 1 individual.</p>
------------------------------------	--

<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>• Requested the unintended recipient destroy the email.</li> <li>• Spoke with the employee who sent the errant email about the importance of protecting personal information.</li> <li>• Requested each employee complete a review of PIPA by July 15, 2020.</li> <li>• All employees will document, review, and sign-off confidential information.</li> </ul>
---	---

<p><b>Steps taken to notify individuals of the incident</b></p>	<p>The affected individual was notified by email on January 12, 2021.</p>
---	---

**REAL RISK OF SIGNIFICANT HARM ANALYSIS**

<p><b>Harm</b> 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 reported,</p> <p style="text-align: center;"><i>Financial information for the student was shared with another student in the same class and if released could be used maliciously to cause mental and emotional harm as well as damage to their reputation which would force them to leave our program.</i></p> <p>In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause hurt,</p>
--	--

	<p>humiliation and embarrassment, as well as damage to reputation. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.</p>
<p><b>Real Risk</b> 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,</p> <p><i>The person that received the information in error has confirmed she has destroyed the informatin (sic) and will not share any information from the original email. The likely of harm is small as the recipients have gone through our organization's lengthy (sic) screening process to be admitted to our training programs and any attempts at creating harm for others would remove them from our program.</i></p> <p>In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error, the recipient is known to the Organization, reported the breach and confirmed the information was deleted. However, the fact the unintended recipient and the affected individual are students in the same class increases the likelihood the harms of hurt, humiliation and embarrassment, as well as damage to reputation may result.</p>

**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 could be used to cause hurt, humiliation and embarrassment, as well as damage to reputation. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of significant harm resulting from this incident is decreased because the incident did not result from malicious intent, but rather human error, the recipient is known to the Organization, reported the breach and confirmed the information was deleted. However, the fact the unintended recipient and the affected individual are students in the same class increases the likelihood the harms of hurt, humiliation and embarrassment, as well as damage to reputation may result.

I require the Organization to notify the affected individual, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by email on January 12, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton  
Information and Privacy Commissioner