



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

<b>Organization providing notice under section 34.1 of PIPA</b>	Water Environment Federation (Organization)
<b>Decision number (file number)</b>	P2017-ND-81 (File #003638)
<b>Date notice received by OIPC</b>	August 5, 2016
<b>Date Organization last provided information</b>	September 9, 2016
<b>Date of decision</b>	June 19, 2017
<b>Summary of decision</b>	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).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is a not-for-profit technical and educational organization; however, it is not a “non-profit organization” as defined in section 56(1)(b) of PIPA. The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved the following:</p> <ul style="list-style-type: none"><li>• name,</li><li>• address,</li><li>• telephone number,</li><li>• payment card information (including payment card number and CVV code, if provided).</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information may have been collected in Alberta and is about residents of Alberta.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>• The Organization uses a third party vendor to assist with its membership renewal outreach.</li> <li>• On June 27, 2016, the vendor informed the Organization that an unauthorized individual gained access to the vendor’s system on April 24, 2016, and deleted membership information that was collected between August 17, 2015 and April 24, 2016.</li> <li>• The vendor reported that its investigation did not reveal any evidence that the personal information was accessed or acquired by the unauthorized individual.</li> </ul>
<p><b>Affected individuals</b></p>	<p>The incident affected five (5) individuals in Alberta.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>• The vendor launched an investigation to determine whether a security incident had occurred.</li> <li>• Reported the matter to law enforcement.</li> <li>• Terminated relationship with the vendor.</li> <li>• Offered affected individuals independent credit monitoring services for 12 months.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>The Organization reported that all affected individuals were notified by letter by July 14, 2016.</p>
<p><b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b></p>	
<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 did not specifically assess the type of harm that might result from this incident, although its notice to affected individuals said “We have not been made aware of any reports of fraud in connection with this incident. Nevertheless, we encourage you to carefully review your credit card statement for unauthorized charges.”</p> <p>In my view, the financial information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. 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 that it “believes the risk of harm to impacted individuals is low, primarily because there is no evidence to suggest that the payment card information was accessed, let alone acquired, as a result of the incident. Moreover, [the Organization] has not received any reports of misuse of the data of impacted members. In addition, under the terms of their cardholder agreement with their respective card issuers, members have zero liability for any unauthorized use of their credit card number.”</p>

	<p>In my view, there is a real risk of harm resulting from this incident. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired or accessed. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.</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 individuals. The financial information involved in this incident could be used to cause the significant harms of identity theft, fraud and financial loss. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired or accessed. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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

I understand all affected individuals were notified by letter by July 14, 2016. The Organization is not required to notify affected individuals again.

Jill Clayton  
Information and Privacy Commissioner