Office of the Information and
Privacy Commissioner of Alberta

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

| | |
|---|---|
| **Organization providing notice under section 34.1 of PIPA** | NAFSA: Association of International Educators (Organization) |
| **Decision number (file number)** | P2020-ND-196 (File # 017100) |
| **Date notice received by OIPC** | August 19, 2020 |
| **Date Organization last provided information** | September 23, 2020 |
| **Date of decision** | February 23, 2021 |
| **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 individual whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA). |
| **JURISDICTION** | |
| **Section 1(1)(i) of PIPA "organization"** | The Organization is an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved the following information of an Alberta resident:<br><br>• name,<br>• address,<br>• payment card number, expiry date, and security code.<br><br>This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's online store (https://shop.nafsa.org/) checkout page. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • The Organization discovered that an unauthorized third party may have gained access to customer information entered into form fields on its online store (https://shop.nafsa.org/) checkout page between April 8, 2020 and May 15, 2020. |

| | |
|---|---|
| **Affected individuals** | The incident affected 22 individuals in Canada, including one individual residing in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Immediately took the affected system offline.<br>• Restored the online store environment with new hardware.<br>• Confirmed a copy of the data was free of compromise.<br>• Worked with cybersecurity experts to determine the root cause of the compromise, whether sensitive data was accessed and whether any evidence of unauthorized access still exists.<br>• Offered affected individuals one year of free credit monitoring and identity theft prevention services.<br>• Notified the Cyber Crime division of the US Federal Bureau of Investigation.<br>• Notified relevant credit payment card companies of the incident.<br>• Notified the Office of the Privacy Commissioner of Canada, the Offices of the Information and Privacy Commissioners of Alberta and British Columbia and the Commission d'accès à l'information du Québec. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on August 21, 2020. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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 did not specifically identify the types of harm(s) that might result from this incident, but reported it "… is taking steps to send notifications to all affected individuals in Canada directly and will be offering affected individuals one-year of free credit monitoring and identity theft prevention services".<br><br>In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. |
| **Real Risk**<br>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. | The Organization did not report its assessment of the likelihood of harm resulting from this incident; however, it reported that it "…notified the Cyber Crime division of the US Federal Bureau of Investigation and relevant payment card companies of the incident in order to prevent fraudulent activity from occurring".<br><br>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. Further, it appears the information was exposed for approximately 1 month. |

| 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.<br><br>A reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. Further, it appears the information was exposed for approximately 1 month.<br><br>I require the Organization to notify the affected individual whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).<br><br>I understand the Organization notified affected individuals by letter on August 21, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again. |

Jill Clayton
Information and Privacy Commissioner