



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

|  |  |
|--|--|
| <b>Organization providing notice under section 34.1 of PIPA</b>  | Hanna Andersson, LLC (Organization)  |
| <b>Decision number (file number)</b>   | P2020-ND-074 (File # 014975)   |
| <b>Date notice received by OIPC</b>  | February 10, 2020  |
| <b>Date Organization last provided information</b>   | February 10, 2020  |
| <b>Date of decision</b>  | July 17, 2020  |
| <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 whose personal information was collected in Alberta 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 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 information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• shipping address,</li><li>• billing address,</li><li>• payment card number, security code, and expiry date.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected via the Organization’s ecommerce website.</p> |
| <b>DESCRIPTION OF INCIDENT</b>   |  |
| <input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure |  |
| <b>Description of incident</b>   | <ul style="list-style-type: none"><li>• On December 5, 2019, law enforcement informed the Organization that credit cards used on its website were available for purchase on a dark web site.</li></ul>   |

|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>• The Organization investigated, and confirmed its third-party ecommerce platform, Salesforce Commerce Cloud, was infected with malware that may have scraped information entered by customers into the platform during the purchase process.</li> <li>• The earliest potential date of compromise identified by forensic investigators is September 16, 2019, and the malware was removed on November 11, 2019.</li> </ul>   |
| <b>Affected individuals</b>  | The incident affected 231 individuals in Alberta.  |
| <b>Steps taken to reduce risk of harm to individuals</b>   | <ul style="list-style-type: none"> <li>• Cooperating with law enforcement and payment card brands.</li> <li>• Card brands have replaced cards involved in fraudulent charges. All consumers potentially affected have been notified.</li> <li>• Took steps to re-secure the online purchasing platform and further harden it against compromise.</li> </ul>  |
| <b>Steps taken to notify individuals of the incident</b>   | Affected individuals were notified by letter on February 10, 2020.   |
| <b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>  |  |
| <p><b>Harm</b><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.</p> | <p>The Organization reported “Harm to individuals is unlikely. Misuse of credit card information is possible, but consumers are unlikely to be responsible for charges.”</p> <p>In my view, a reasonable person would consider the financial information at issue could be used to cause the significant harms of identity theft and fraud.</p>  |
| <p><b>Real Risk</b><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.</p>                             | <p>The Organization reported “Harm to individuals is unlikely. Card brands have identified fraudulent charges [sic] related to fewer than .01% of potentially affected customers.”</p> <p>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. It appears the information was exposed for almost 2 months and some fraud has occurred. 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.

A reasonable person would consider the 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. It appears the information was exposed for almost 2 months and some fraud has occurred. 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 whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter on February 10, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner