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** | IMI Precision Engineering d/b/a Bimba Manufacturing (Organization) |
| **Decision number (file number)** | P2021-ND-236 (File #018838) |
| **Date notice received by OIPC** | January 4, 2021 |
| **Date Organization last provided information** | January 4, 2021 |
| **Date of decision** | November 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 individuals 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 manufactures and sells heavy equipment (hydraulic, pneumatic and electrical) to business customers. The Organization's head office is located in Illinois, USA.<br><br>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 some or all of the following information:<br><br>• name,<br>• business contact information, and<br>• credit card information (expiry date and security code).<br><br>The Organization reported, "the three Albertans whose information was compromised were customers who purchased … products in a B2B context" and that the addresses of the affected individuals in Alberta are business addresses of companies.<br><br>As such, some of the information may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." |

| | |
|---|---|
| | Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose."<br><br>In this case, I considered that the possible unauthorized disclosure of the information at issue was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies to the business contact information (name and address).<br><br>The Organization also reported, "…in some cases the companies appear to be small businesses, and in no case is it possible to tell if the credit card used was a company card or a personal card, and thus it is not certain which, if any, of the information compromised would qualify as "personal information" within the meaning of applicable [sic]."<br><br>To the extent the information at issue is about identifiable individuals, it is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On November 20, 2020, the organization's vendor was informed that the vendor's service provider had a vulnerability on the server(s) that hosted one of the Organization's websites, Bimba.com.<br>• As a result, an unauthorized user may have been able to access or acquire the personal information of the Organization's customers.<br>• The unauthorized user inserted malicious code into web files causing unencrypted copies of e-commerce transaction data to be diverted to the unauthorized user.<br>• The information may have been exposed between August 21, 2020 and November 13, 2020. |
| **Affected individuals** | The incident affected 844 individuals, including three (3) Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Investigated and reviewed the potentially affected records.<br>• Monitored the website daily. |

| | |
|---|---|
| | • Worked closely with payment card companies.<br>• Determined the scope of the incident and arranged for a two-year identity theft protection services for affected individuals.<br>• Encouraged affected individuals to take preventative measures.<br>• Creating and implementing additional security measures, internal controls, and safeguards, as well as continuing to make changes to existing policies and procedures designed to prevent a similar occurrence. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on December 24, 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 reported the possible harms that may occur as a result of the breach are "Identity theft, financial harms."<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and financial harm. |
| **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 reported, "Given that credit card information was compromised, there is a reasonable risk of serious harm."<br><br>In my view, the likelihood of harm is increased because the incident resulted from the deliberate action of an unknown perpetrator(s) indicating malicious intent, and the information may have been exposed for approximately two and a half months. |
| **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 that the contact and financial information at issue could be used to cause the significant harms of identity theft and financial harm. The likelihood of harm is increased because the incident resulted from the deliberate action of an unknown perpetrator(s) indicating malicious intent, and the information may have been exposed for approximately two and a half months.<br><br>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 the affected individuals by letter dated December 24, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner