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** | OrthoAccel Technologies, Inc. (Organization) |
| **Decision number (file number)** | P2020-ND-012 (File #013730) |
| **Date notice received by OIPC** | October 22, 2019 |
| **Date Organization last provided information** | October 22, 2019 |
| **Date of decision** | February 13, 2020 |
| **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 is an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The information at issue includes name, and credit or debit card information.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On or about January 14, 2019, the Organization became aware of suspicious activity relating to certain employee email accounts.<br>• On January 28, 2019, the Organization's investigation confirmed one of its email account users was the victim of a phishing event that resulted in unauthorized access to their email account on separate occasions between December 6, 2018 and January 14, 2019. |

| | |
|---|---|
| | • On February 4, 2019, the investigation confirmed two additional email account users were subject to unauthorized access on separate occasions between December 4, 2018 and January 27, 2019. |
| **Affected individuals** | The incident affected 1 individual in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Worked with third-party forensic investigators to determine the nature and scope of the incident.<br>• Undertook a programmatic and manual review of the email accounts to identify potentially affected personal information.<br>• Assessed the security of systems, reset relevant passwords, and working to implement additional safeguards and training to its employees.<br>• Reported the incident to U.S. law enforcement and other regulators. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by mail on October 9, 2019. |
| **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 potential harm(s) that might result from the incident but reported that it "…is providing impacted individuals with guidance on how to better protect against identity theft and fraud…".<br><br>In my view, a reasonable person would consider that the 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 provide an assessment of the likelihood of harm resulting from this incident.<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, phishing) that occurred repeatedly over the course of almost two months before being detected. |
| **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 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 as the breach was the result of malicious intent (deliberate action, phishing) that occurred repeatedly over the course of almost two months before being detected.

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 individuals notified by mail on October 9, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner