



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|--|--|
| Organization providing notice under section 34.1 of PIPA | Atria Senior Living (Organization) |
| Decision number (file number) | P2020-ND-125 (File #013992) |
| Date notice received by OIPC | November 20, 2019 |
| Date Organization last provided information | November 20, 2019 |
| Date of decision | October 27, 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 <i>the Personal Information Protection Act</i> (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” | <p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• date of birth,• Social Insurance Number, and/or• limited medical information. <p>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.</p> |
| DESCRIPTION OF INCIDENT | |
| <input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure | |
| Description of incident | <ul style="list-style-type: none">• On October 24, 2019, the Organization identified suspicious activity related to certain employee email accounts. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • The Organization’s investigation of the email phishing incident showed that an unauthorized person first had access to an employee's email account on September 18, 2019 and last had access on September 20, 2019. • The investigation was unable to determine which specific emails or attachments, if any, were viewed by the unauthorized person. |
| Affected individuals | The incident affected 10,509 individuals, including 8 in Alberta. |
| Steps taken to reduce risk of harm to individuals | <ul style="list-style-type: none"> • Secured the accounts and investigated with the assistance of a cybersecurity firm. • Offered affected individuals complimentary, one-year credit monitoring and identity theft prevention. |
| Steps taken to notify individuals of the incident | Affected individuals were notified by letter on November 19, 2019. |
| REAL RISK OF SIGNIFICANT HARM ANALYSIS | |
| <p>Harm 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 “Stolen social insurance numbers can be used to commit identity theft.”</p> <p>In my view, a reasonable person would consider the identity information at issue could be used to cause the significant harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment.</p> |
| <p>Real Risk 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 did not specifically provide an assessment of the likelihood of harm resulting from this incident, but reported it “... is offering eligible individuals a complimentary, one-year membership to ...credit monitoring and identity theft prevention. To further diminish the likelihood of harm, [the Organization] is recommending that the individuals involved closely review their financial and/or medical statements for any unauthorized activity.”</p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it resulted from malicious action (deliberate, phishing attack).</p> |
| DECISION UNDER SECTION 37.1(1) OF PIPA | |
| <p>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.</p> <p>A reasonable person would consider the identity information at issue could be used to cause the significant harms of identity theft and fraud. Medical information could be used to cause the harms of</p> | |

hurt, humiliation and embarrassment. The likelihood of harm resulting from this incident is increased because it resulted from malicious action (deliberate, phishing attack).

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 affected individuals were notified by letter on November 19, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner