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** | Chamberlain Group, Inc. (Organization) |
| **Decision number (file number)** | P2019-ND-035 (File #013320) |
| **Date notice received by OIPC** | May 29, 2019 |
| **Date Organization last provided information** | May 29, 2019 |
| **Date of decision** | March 9, 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 those 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 incident involved all or some of the following information:<br>• name,<br>• address,<br>• payment card number, expiry date, and security code.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information at issue was collected by a call center in Arizona. To the extent this information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On April 28, 2019, the Organization discovered that a call center employee had not followed mandated security procedures when handling customer payment card information. |

| | |
|---|---|
| | • Upon notification from law enforcement that the employee had apparently misused the payment card information of other individuals, the Organization investigated.<br>• The investigation found that the employee had collected personal information from some Alberta residents between November 2, 2018 through April 24, 2019.<br>• The Organization found no information indicating that the former employee mishandled or misused the Alberta residents' personal information.<br>• Out of an abundance of caution, the Organization decided to notify all customers whose payment card information had been handled by this former employee during employment at the Organization. |
| **Affected individuals** | The incident affected 137 individuals, including 2 residents of Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Conducted an investigation.<br>• The employee is no longer employed with the Organization and was reported to law enforcement.<br>• Reported incident to payment card companies.<br>• Offered affected Alberta residents an identity theft protection product.<br>• Introducing an enhanced process for most call centre payment card transactions such that call center employees do not access payment card information.<br>• Reviewing security policies to identify areas for improvement.<br>• Looking into opportunities for additional training to prevent a recurrence. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on May 24, 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 report it "…found no information indicating that the former call center employee had actually misused Alberta customers' payment card information. Nevertheless, we cannot rule out the possibility that the former call center employee misused Alberta customers' payment card information, for example, by using the information to make an unauthorized purchase."<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, including to make unauthorized purchases. |

| | |
|---|---|
| **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 "We think the risk is very low. Even if there were unauthorized purchases, the relevant payment card companies … have committed to protect card users against financial loss for unauthorized transactions."<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 deliberate action (rogue employee copying down personal information) and was potentially at risk for approximately 5 months. The Organization did not report on any efforts to ensure all information was recovered, or to confirm that it had not been used or further disclosed. The Organization can only speculate that affected individuals may 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. |

**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 that the financial information at issue could be used to cause the significant harms of identity theft and fraud, including to make unauthorized purchases. The likelihood of harm resulting from this incident is increased as the breach was the result of deliberate action (rogue employee copying down personal information) and was potentially at risk for approximately 5 months. The Organization did not report on any efforts to ensure all information was recovered, or to confirm that it had not been used or further disclosed. The Organization can only speculate that affected individuals may 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 in a letter dated May 24, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner