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** | car2go NA, LLC and car2go Canada Ltd. dba as SHARE NOW (Organization) |
| **Decision number (file number)** | P2020-ND-193 (File #016281) |
| **Date notice received by OIPC** | June 29, 2020 |
| **Date Organization last provided information** | June 29, 2020 |
| **Date of decision** | December 16, 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's head office is in Austin, Texas, USA. The Organization commenced operations in Canada in 2011 and ceased operations in Canada on February 29, 2020. The Organization's former customers in Canada can access their password-protected SHARE NOW accounts using the SHARE NOW mobile application.<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 all or some of the following information:<br><br>• first and last name,<br>• postal address.<br>• email address,<br>• last four digit only of telephone number,<br>• date of trip, car model, cost, start point, end point, minutes of usage,<br>• invoice, and<br>• last four digits of credit card number.<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 May 20, 2020, an unauthorized third party(ies) used North American IP addresses to perpetrate a "brute force" attack against the Organization's online customer account system.<br>• The attacker made repeated trial-and-error attempts to log into the Organization's online customer accounts using email addresses combined with hundreds or possibly thousands of passwords.<br>• Some of the email addresses used by the attacker belong to the Organization's customers and former customers but other email addresses do not, which indicates that the attacker used lists of email addresses obtained from another source (e.g. the dark web).<br>• The Organization reported that it does not know if the attacker used passwords that were guessed or were compromised authentic passwords used for online services unconnected with the Organization.<br>• On May 25, 2020, the Organization determined that the attacker accessed two (2) accounts belonging to two (2) former customers, both of whom reside in Alberta.<br>• The Organization said that while the attacker was able to access the accounts, it does not know whether the attacker actually accessed the personal information in the accounts. |
| **Affected individuals** | The incident affected two (2) individuals residing in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Detected, contained, investigated and resolved the incident.<br>• Implemented technological counter-measures specific to the IP addresses used by the attacker.<br>• Implemented technological measures designed to allow former customers in North America to continue to remotely access their accounts while protecting those accounts against brute force (email address and password guessing) attacks.<br>• Provided former customers with information regarding additional steps they could take to protect themselves and their personal information.<br>• Offered the two affected individuals a 12-month subscription to an identity theft and credit monitoring service free of charge. |

| | |
|---|---|
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email on June 29, 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:<br><br>*Based on the nature of the incident, the possible harms that might occur as a result of the breach could include fraud/phishing emails, identity theft and use of account credentials (i.e. email and password) to attempt to access other online services and apps.*<br><br>I agree with the Organization's assessment. A reasonable person would consider that, particularly when combined with profile information (e.g. information that individuals are customers of the Organization), individual names and email addresses could be used to send sophisticated, user-specific emails purportedly from the Organization (phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks), including an increased vulnerability to identity theft and fraud. Finally, there may be a security/safety risk as a result of trip details being involved in the incident. These are all significant harms. |
| **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 that it "…is not aware of any actual or attempted misuse of its former customers' personal information, and has no indication that any harm to its former customers has occurred as a result of the incident...".<br><br>Further, "In light of the nature of the personal information contained in the accounts (i.e. low sensitivity information that relates to … trips that occurred more than one year before the breach), the limited number of individuals involved (only two), and uncertainty as to whether the personal information in the accounts was actually accessed, [the Organization] is of the view that the breach does not present any real risk of significant harm to any individual."<br><br>In my view, the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a third party. The Organization reported that the attacker accessed the accounts but does not know whether the attacker accessed the personal information in the accounts. Although the trips occurred more than one year before the breach, the lack of reported incidents resulting from this breach to date is not a mitigating |

| | |
|---|---|
| | factor, as phishing, identity theft and fraud can occur months and even years after a data breach. |

**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, particularly when combined with profile information (e.g. information that individuals are customers of the Organization), individual names and email addresses could be used to send sophisticated, user-specific emails purportedly from the Organization (phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks), including an increased vulnerability to identity theft and fraud. Finally, there may be a security/safety risk as a result of trip details being involved in the incident. These are all significant harms.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a third party. The Organization reported that the attacker accessed the accounts but does not know whether the attacker accessed the personal information in the accounts. Although the trips occurred more than one year before the breach, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

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 an email dated June 29, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner