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** | Nissan Canada Inc. (Organization) |
| **Decision number (file number)** | P2021-ND-294 (File #019905) |
| **Date notice received by OIPC** | March 9, 2021 |
| **Date Organization last provided information** | October 15, 2021 |
| **Date of decision** | March 2, 2022 |
| **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>• vehicle identification number (VIN),<br>• city and province of residence (but not street address), and postal code.<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** | • The Organization is an affiliate of Nissan North America, Inc. ("Nissan NA"); the latter provides administrative services, including information technology services, to the Organization, and also provides a suite of connected vehicle services known as Nissan ConnectServices (and for the INFINITI brand, known as INFINITI InTouch Services) that allows vehicle owners to |

| | |
|---|---|
| | access vehicle information, stay connected to their vehicle, and get assistance when they need it.<br>• On January 2, 2021, the Organization became aware it was the victim of a data breach that may have involved unauthorized person(s) gaining access to information of customers who, between November 17, 2020 and January 5, 2021, were enrolled in the NissanConnect Services or INFINITI InTouch Services.<br>• On January 5, 2021, the internal Global Alliance Security Team advised Nissan NA that the source code from a server had been accessed by unauthorized persons.<br>• The Organization reported the perpetrators appear to have used elements in the exposed source code to gain further access to a server that contained the information at issue.<br>• On January 15, 2021, all compromised credentials were remediated. |
| **Affected individuals** | The incident affected approximately 33,000 Canadians, including 5,574 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Took the server offline; retained a third party cybersecurity team to assist with investigation and remediation.<br>• Contacted the perpetrator who first exposed the source code, and it was removed from the public domain.<br>• Provided affected individuals with 12 months of credit monitoring services without charge.<br>• Contacted law enforcement, and provincial privacy regulators in British Columbia, Alberta and Quebec.<br><br><u>Nissan NA</u><br>• Executed its security incident response procedures and investigation activities.<br>• Completed password resets for all system service accounts.<br>• Performed a security review and audit of its security monitoring software.<br>• Performed additional automated and manual scans/reviews for vulnerabilities.<br>• Expanded threat monitoring.<br>• Contracted a third party security specialist to perform an independent audit as well as "dark web" threat and activity monitoring. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter and email on or about March 8 and 9, 2021. |

| 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 any harms that might result from this incident, but its notification to affected individuals stated,<br><br>*We understand that you may feel uneasy. Out of an abundance of caution and to provide you additional confidence, we are offering you 12 months of credit monitoring services …at no cost.*<br><br>*We are not aware of any reports of identity theft or other fraud related to this incident. If you believe your information was used for fraudulent purposes, we strongly recommend you contact your local police department and the Canadian Anti-Fraud Centre...*<br><br>In my view, a reasonable person would consider the contact and vehicle information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. |
| **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 "…believes the risk to affected consumers to be small."<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. In addition, the information was available to the perpetrator for approximately 7 weeks. |

**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 the contact and vehicle information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. In addition, the information was available to the perpetrator for approximately 7 weeks.

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 by email and letter on or about March 8 and 9, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner