Nissan Motor Co. Australia
Nissan Financial Services Australia

Notice: Cyber security incident impacting Nissan Australia and New Zealand

Nissan Financial Services Australia Pty Ltd, Nissan Motor Co. (Australia) Pty Ltd, Nissan Financial Services New Zealand Pty Ltd and Nissan New Zealand Ltd (***Nissan***) experienced a cybersecurity incident that has affected the personal information of some of our customers, staff and other stakeholders.

This notification outlines what has happened, how you may be personally affected and advice on what to do. We encourage you to read this information carefully to understand what it may mean for you and how Nissan is supporting you.

We are very sorry this has happened, and we sincerely apologise for any upset this notice might cause.

Nissan cyber incident

On 5 December 2023, Nissan experienced a cyber-incident that involved a malicious third party gaining unauthorised access to Nissan's Australia and New Zealand IT servers. We acted immediately to contain the breach and began working with our global incident response team and cybersecurity experts to understand what information was accessed and which individuals are affected.

Our investigation has revealed that unfortunately, the personal information of some of our customers, staff and other stakeholders was stolen and published on the dark web as a result of the incident.

OracleCMS cyber incident

Regrettably, we recently became aware of a second data breach that occurred with one of our suppliers, and which has also impacted some individuals whose information was compromised during the Nissan cyber incident.

As part of Nissan's incident response, a dedicated call centre was established to help manage customer enquiries. This was outsourced to an external call centre operator, OracleCMS. OracleCMS was provided with summary information to help answer questions from people who received a breach notification letter from us.

OracleCMS subsequently suffered a data breach, which it was alerted to on 15 April 2024. This separate incident resulted in certain data which was held by OracleCMS, including the summary information Nissan provided to OracleCMS, being compromised and published on the dark web.

This means that, for individuals affected by both the Nissan breach and subsequent OracleCMS breach:

1. their personal information was unlawfully accessed from Nissan's IT servers on 5 December 2023; and
2. a summary description of the personal information that was compromised in the December incident was also published on the dark web as a result of the OracleCMS data breach.

Why does Nissan hold personal information?

Nissan provides service and customer support for various Nissan vehicles as well as a range of finance products and insurance products under other business names, including Nissan Financial Services, Nissan Insurance, Mitsubishi Motors Financial Services, Skyline Car Finance, Skyline Car Insurance, Renault Financial Services, Renault Insurance and Infiniti Financial Services. This notice may apply to you even if you did not obtain Nissan-branded finance or insurance.

Nissan also holds personal information about individuals who have (or individuals who are related to a person or a business who has) bought or serviced a vehicle with Nissan, obtained finance or insurance from Nissan or one of the brands listed above. Alternatively, it may also apply to you if you currently work at or at some stage worked at, or with, Nissan. This notification may apply to you even if you did not obtain Nissan-branded finance or insurance, and you have not worked at or with Nissan.

Who this notice is for?

Nissan is providing notifications directly to affected individuals who have been identified as requiring notification and where Nissan holds current contact information for those individuals. Wherever possible, individuals will be provided with a direct notification. If an individual has been impacted by both the Nissan and OracleCMS incidents, we will endeavour to directly notify people of this as well.

If you have received a notification directly from Nissan (in connection with either incident), please refer to that notice, which contains information specific to you as to what personal information was impacted, as well as a unique code to gain access to the support services that have been made available to you.

Some affected individuals who Nissan has identified as requiring notification have not been able to be contacted using available contact details. This notice is relevant to those individuals.

Details of the types of personal information that has been affected

Nissan cyber incident

In respect of the Nissan cyber incident, the following list describes the type of personal information that may have been impacted. Please note that not all of the information below applies to every person who was impacted:

- names;
- contact details, including address, telephone numbers and email addresses;
- dates of birth
- copies of identity documents or other government issued identifiers or certifications supplied by individuals to Nissan, which includes drivers licences, Medicare cards, passports, visas and right to work details, concession/Proof of Age cards, Centrelink income statements, birth certificates, marriage certificates, immigration cards, citizenship certificates, NZ national health index numbers;
- government identifiers (including drivers licence numbers, Medicare card numbers, visa numbers and passport numbers), which were sometimes recorded by Nissan in addition to or separate from a copy of the relevant identity document;
- Australian Tax File Numbers or New Zealand IRD Numbers;
- Sensitive information (which may include health information or medical information; police check / criminal record information; sexual orientation / practices; religious beliefs; trade union / professional organisation membership);
- information related to a person's credit, generally relating to an auto-finance relationship with Nissan (which may include an individual's default listing or default notices, credit default information, dishonour notice or letter, credit report or credit check, repossession information, bankruptcy information or debt agreement proposal),
- financial information (including credit card information or bank account information);
- vehicle registration details and information about a Nissan car loan, including your transaction history and information about your loan repayment history;
- information relating to an individual's employment, either with Nissan, or provided to Nissan in connection with their relationship Nissan. This may include salary information, performance assessments / evaluations, employment application information, professional or occupational documents ,employment contracts, workplace incident or investigation reports and termination or redundancy notices)
- details of superannuation or insurance arrangements (including payments/policy, fund and membership details).

OracleCMS cyber incident

In respect of the OracleCMS cyber incident, the following information has been impacted. As with the Nissan cyber incident, the exact combination of this personal information varies for each individual:

- names;
- contact details, including address, telephone numbers and email addresses;
- dates of birth; and
- bank account information. This information was only present for individuals who sought re-imbursement for ID document replacement through Nissan's call centre.

Support services for affected individuals

We have notified, and are keeping updated as and when required, law enforcement bodies and government agencies including:

- the Australian Cyber Security Centre;
- the Office of the Australian Information Commissioner;
- the Australian Taxation Office;
- other relevant regulators, law enforcement bodies and government agencies.

We have also put in place a number of services to minimise the risk of identity theft, scams or fraud for those who have been affected:

1. **Equifax credit monitoring**

We have partnered with Equifax to offer 12 months' free access to Equifax Protect for individuals who have had core identity documentation or other important personal information been impacted.

Equifax Protect is a credit and identity monitoring service, designed to help safeguard individuals from fraud and financial loss in the event of a data breach.

If you think you have been affected and you would like to access Equifax Protect you can contact Nissan's dedicated support line via the details set out below.

We also recommend that you:

- monitor your credit reports, bank accounts and government accounts to ensure that there is no unexpected or unauthorised activity occurring;

- notify the Australian Taxation Office in respect of the potential compromise of your tax file number;
- monitor online accounts for unusual activity, and not open any suspicious texts, pop-up windows or emails, and not click on suspicious links or open unusual attachments.

2. **IDCARE identity support services**

Nissan has partnered with IDCARE, Australia's national identity and cyber support community service.

They have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused.

If you believe that you have been affected by this incident, IDCARE's services are at no cost to you. You can contact our dedicated support line via the details set out below to get more information about how you can access IDCARE's services using Nissan's access code.

3. **Reimbursement for replacement of government-issued identification**

If your primary identity documents (for example, your driver's licence, proof of age card or passport) have been affected by the Nissan cyber incident and the advice from the issuing government agency is to replace that document, Nissan will reimburse you for the cost of any replacement.

If you are concerned that your primary identity documents have been compromised, you can contact our dedicated support line via the details set out below.

What else you can do

In addition to our core support services set out above, we recommend that anyone potentially affected by this incident takes the following steps to help safeguard against malicious online activity:

- monitor your online accounts for unusual activity and do not open any suspicious texts, pop-up windows, emails or attachments, or click on any suspicious links;
- contact the Australian Taxation Office if you have any concerns regarding the security of your MyGov account;
- obtain a free credit report to check for suspicious activity, which could help identify any misuse of your personal information. You can obtain a free credit report once every three months from the following credit reporting bodies:
    - Centrix – (if you live in New Zealand 0800 236 874);

    - Equifax – (if you live in Australia 13 83 32, or if you live in New Zealand 0800 692 733);
    - illion – (if you live in Australia 1300 734 806, or if you live in New Zealand 0800 733 707); or
    - Experian – (if you live in Australia 1300 783 864);
- be vigilant for any unusual or suspicious online activity;
- be vigilant for any unrecognised or unsolicited telephone calls, emails or messages asking you to provide personal information;
- update your passwords for your online accounts;
- enable multi-factor authentication for your online accounts where possible; and
- avoid clicking on any links or opening any suspicious emails or attachments.

How to contact us

If you are a Nissan customer, or customer of one of businesses listed above and are concerned about whether your personal information has been impacted, you can contact our dedicated support line on 1800 958 000 (if you live in Australia) or 0800 445 014 (if you live in New Zealand). This contact centre operates between 7:00am – 7:00pm AEST weekdays (excluding public holidays).

Again, we are very sorry if this incident has affected you personally.