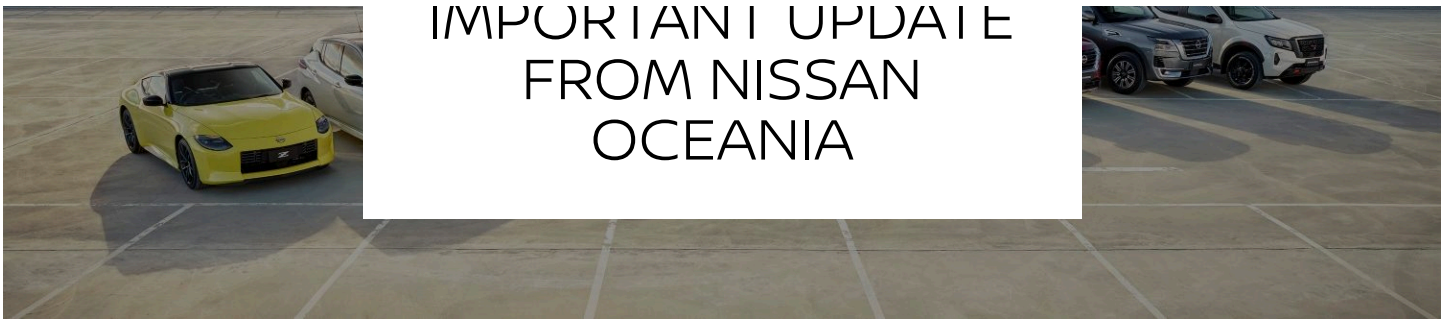

IMPORTANT UPDATE FROM NISSAN OCEANIA

The Australian and New Zealand Nissan Corporation and Financial Services (“Nissan”) is currently managing a cyber incident. Here is the latest information on our incident response.

Updated Wednesday, 13 March 2024

The Nissan Motor Corporation and Nissan Financial Services in Australia and New Zealand ("Nissan Oceania") has today begun contacting individuals in relation to a cyber incident that has affected its local businesses.

On 5 December 2023, a malicious third party obtained unauthorised access to our local IT servers. We took immediate action to contain the breach, and promptly alerted the relevant government authorities, including the Australian and New Zealand national cyber security centres and privacy regulators.

Since that time, Nissan has been working urgently with government authorities and external cyber forensic experts to review the compromised data and understand the impact on individuals within our community.

We now know the list of affected individuals includes some of Nissan's customers (including customers of our Mitsubishi, Renault, Skyline, Infiniti, LDV and RAM branded finance businesses), dealers, and some current and former employees.

Nissan expects to formally notify approximately 100,000 individuals about the cyber breach over the coming weeks. This number might reduce as contact details are validated and duplicated names are removed from the list.

The type of information involved will be different for each person. Current estimates are that up to 10% of individuals have had some form of government identification compromised. The data set includes approximately 4,000 Medicare cards, 7,500 driver’s licenses, 220 passports and 1,300 tax file numbers.

The remaining 90% of individuals being notified have had some other form of personal information impacted; including copies of loan-related transaction statements for loan accounts, employment or salary information or general information such as dates of birth.

We know this will be difficult news for people to receive, and we sincerely apologise to our community for any concerns or distress it may cause.

We are committed to contacting affected individuals as soon as possible to tell them what information was involved, how we are supporting them, and the steps they can take to protect themselves against the risk of harm, identity theft, scams or fraud.

Support and guidance for affected individuals

Nissan has put in place a number of services to support individuals who have had personal information compromised. This includes access to IDCARE, free credit monitoring, and reimbursement where the replacement of government ID is recommended by the relevant issuing authority.

The following measures will be available depending on a person's individual circumstances:

- **IDCARE:** We have partnered with IDCARE, Australia and New Zealand's national identity and cyber support community service. IDCARE's expert case managers will work with impacted individuals to address any concerns about risks to their personal information, and any instances where they think information might be misused. IDCARE's services are available at no cost to those affected by the cyber incident.
- **Equifax:** In Australia, we are providing free access to Equifax credit monitoring services for 12 months to watch for any fraudulent activity.
- **Centrix:** In New Zealand, we are providing customers with free access to Centrix to assist with the provision of a credit report and placement of a credit freeze on their credit file.
- **ID replacement:** Where someone's primary identity documents have been compromised, and the advice from the issuing government agency is to replace the document, Nissan will reimburse the cost of the replacement.
- **Customer support line:** We have established a dedicated customer support line for individuals who have received an email or letter notification. They can be contacted between 7am and 7pm AEDT weekdays on:
  - **Australia** 1800 958 000
  - **New Zealand** 0800 44 50 14

Additional advice to protect against identity theft, scams or fraud:

In addition to the above measures, we continue to encourage everyone to take the following steps:

- Be vigilant for any unusual or suspicious online activity.
- Avoid clicking on any links or opening any suspicious emails or attachments.
- Be vigilant for any unrecognised or unsolicited telephone calls, emails or messages asking you to provide personal information.
- Always verify the sender of any communications received to make sure they're legitimate.
- Update your passwords regularly, using 'strong' passwords and not re-using passwords for multiple accounts.
- Enable multi-factor authentication for your online accounts where available.
- Report a scam in Australia by visiting Scamwatch at www.scamwatch.gov.au.

BACK TO HOMEPAGE

PREVIOUS UPDATES

13 FEB 2024 +

Updated Tuesday, 13 February 2024

The Nissan Motor Corporation and Nissan Financial Services in Australia and New Zealand ("Nissan") continues to investigate a cyber incident that impacted our local IT systems, which resulted in some data being stolen and published on the dark web.

We understand that some of you may be worried about whether the incident has impacted personal information of yours that we hold, and we apologise for any distress this has caused.

Conducting a detailed forensic review of the data takes time. However, please be assured that our team of forensic experts is reviewing and assessing the data as quickly as possible.

Once we have an accurate picture of the compromised data, we will contact affected individuals as needed to let them know what information was impacted, what they can do, and what support is available to them.

At the same time, we encourage everyone to take steps to protect themselves against identity theft, scams or fraud. As a reminder:

- Be vigilant for any unusual or suspicious online activity
- Update your passwords for your online accounts
- Enable multi-factor authentication for your online accounts where possible
- Avoid clicking on any links or opening any suspicious emails or attachments
- Contact IDCare, the Australian and NZ national identity and cyber support service:
  - Australia: 1800 595 160
  - New Zealand: 0800 121 068
- Report a scam in Australia by visiting Scamwatch at www.scamwatch.gov.au
- Request a free credit report from a credit reporting body, if you are in Australia (Equifax, illion and Experian), or from a credit reporting agency if you are in New Zealand (Centrix, Equifax and illion) and check for any applications or requests that you did not make

23 JAN 2024 +

Updated Tuesday, 23 January 2024

The Nissan Motor Corporation and Nissan Financial Services in Australia and New Zealand ("Nissan") is investigating a cyber incident that has impacted our systems.

We can confirm that an unauthorised third party illegally accessed some of Nissan's local systems in Australia and New Zealand and that some of that data has been posted on the dark web.

Our external cyber forensic experts are urgently focused on completing their analysis to determine exactly what information was compromised so that we may notify affected individuals accordingly, and as soon as possible.

The Australian Cyber Security Centre and the New Zealand National Cyber Security Centre continue to assist us with our investigation.

We know this development may be concerning for our Australian and New Zealand customers and we apologise for any distress it has caused.

We are working as quickly as we can to complete our forensic analysis so that we can contact affected individuals as needed, and provide support and assistance where we can.

Regular updates will continue to be posted on the Nissan website. In the meantime, customers with any questions or concerns can contact our dedicated call centre on **+61 3 9000 0814**. This call centre will be staffed between 8:30am – 5:00pm AEDT weekdays (excluding public holidays).

We encourage everyone to continue taking steps to protect themselves against identity theft, scams or fraud, including:

- Be vigilant for any unusual or suspicious online activity
- Update your passwords for your online accounts
- Enable multi-factor authentication for your online accounts where possible
- Avoid clicking on any links or opening any suspicious emails or attachments
- Contact IDCare, the Australian and NZ national identity and cyber support service:
  - Australia: **1800 595 160**
  - New Zealand: **0800 121 068**
- Report a scam in Australia by visiting Scamwatch at www.scamwatch.gov.au
- Request a free credit report from a credit reporting body, if you are in Australia (Equifax, illion and Experian), or from a credit reporting agency if you are in New Zealand (Centrix, Equifax and illion) and check for any applications or requests that you did not make

17 JAN 2024 +

Updated Wednesday, 17 January 2024

We are now aware that some data was accessed in the incident and posted on the dark web. We are working urgently with our global incident response team and cyber forensic experts to understand what information was accessed and the types of information that was posted on the dark web.

Where we identify customer data has been accessed in a manner which gives rise to a risk of serious harm, we will contact you in accordance with our legal obligations, including to let you know what information was involved and what support is available to you.

We have already notified the Australian Cyber Security Centre and the New Zealand National Cyber Security Centre, and the relevant privacy regulators and law enforcement bodies, and we are keeping them updated on our investigation.

We are deeply sorry for any concerns this has caused for those who have been impacted.

Some steps you can take to help safeguard against identity theft, scams or fraud include:

- Be vigilant for any unusual or suspicious online activity
- Update your passwords for your online accounts
- Enable multi-factor authentication for your online accounts where possible
- Avoid clicking on any links or opening any suspicious emails or attachments
- Contact IDCare, the Australian and NZ national identity and cyber support service:
  - Australia: **1800 595 160**
  - New Zealand: **0800 121 068**
- Report a scam in Australia by visiting Scamwatch at www.scamwatch.gov.au
- Request a free credit report from a credit reporting body, if you are in Australia (Equifax, illion and Experian), or from a credit reporting agency if you are in New Zealand (Centrix, Equifax and illion) and check for any applications or requests that you did not make

We will continue to post updates here as they become available. We have established a dedicated contact line to provide updates, which can be contacted on **+61 3 9000 0814**. This contact centre will be staffed between 8:30am – 5:00pm AEDT weekdays (excluding public holidays).

Thank you for your understanding and patience with our team at this time.

11 JAN 2024 +

Updated Thursday, 11 January 2024

Our Build Your Vehicle and Request a Quote functions are now back online and available to use.

Go to SHOP@HOME to browse the Nissan range, choose and customise a vehicle, and request a quote or book a test drive.

4 JAN 2024 +

Updated Thursday, 4 January 2024

Our Nissan Financial Services Customer Portal is now back online and available to use. While it is not required, we recommend you reset your password when you log back in.

We are continuing to work with our global incident response team and cyber forensic experts to understand what information was impacted in the recent cyber incident that impacted our systems.

Conducting a detailed forensic review is an extensive process, which will take some time to complete. We will post weekly updates on our progress here.

We thank you for your understanding and patience as we undertake this necessary work.

22 DEC 2023 +

Updated Friday, 22 December 2023

The Nissan Motor Corporation and Nissan Financial Services in Australia and New Zealand ("Nissan") is investigating a cyber incident that has impacted our systems.

We can now confirm that an unauthorised third party illegally accessed some of the company's network systems in Australia and New Zealand.

We are working urgently with our global incident response team and cyber forensic experts to understand what information was impacted.

We have notified the Australian Cyber Security Centre and the New Zealand National Cyber Security Centre, and the relevant privacy regulators and law enforcement bodies.

Data security is an important priority at Nissan and we are deeply sorry for any concerns this has caused for those who have been impacted.

We will continue to post updates here as they become available. We have established a dedicated contact line to provide updates, which can be contacted on **+61 3 9000 0814**. This contact centre will be staffed between 8:30am – 5:00pm AEDT weekdays (excluding public holidays).

Thank you for your understanding and patience with our team at this time.

21 DEC 2023 +

Updated Thursday, 21 December 2023

The majority of our systems have now returned to normal functionality. Thank you for your patience.

The Nissan Financial Services Customer Portal remains unavailable.

Please contact us via the following call centre numbers:

Nissan Motor Company: 8:30am - 5:30pm AEDT
Australia **1800 035 035** (select option 2)

Nissan Financial Services: 8:30am - 5pm AEDT
Australia **1800 035 035** (select option 3)
New Zealand **0800 463 790**

Please be advised that due to high call and email volumes we are currently experiencing longer than expected delays.

We thank you for your understanding and ask for your patience with our team at this time.

15 DEC 2023 +

Updated Friday, 15 December 2023

All scheduled customer direct debit payments due from the 15th of December 2023 onwards, will be debited in accordance with the terms of your Loan Agreement.

If you had a direct debit payment that was due between the 5th of December and the 14th of December 2023, we will contact you shortly and provide you with two business days' notice prior to debiting your account.

14 DEC 2023 +

Updated Thursday, 14 December 2023

Our call centres are operating with reduced system functionality. We thank you for your understanding and ask for your patience with our team at this time.

12 DEC 2023 +

Updated Tuesday, 12 December 2023

We have now reopened our customer call centres.

Nissan Motor Company customers please call our support team on **1300 812 492** between the hours of 8:30 am - 5:30pm AEDT in Australia and **0800 457 052** in New Zealand.

Nissan Financial Services customers can contact our team on **1300 751 002** between the hours of 8:30 am - 5pm AEDT in Australia and **0800 457 051** in New Zealand.

11 DEC 2023 +

Updated Monday, 11 December 2023

We are aware that customers in Australia and New Zealand are having difficulties contacting us. We are currently working to restore our systems and we will re-establish our customer support phone lines as soon as we can.

We are continuing to investigate the cyber incident and we will provide further updates as soon as possible.

We also want to reassure customers the systems outage will not adversely impact the credit rating of any of our Nissan Financial Services customers.

5 DEC 2023 +

Tuesday, 5 December 2023

The Australian and New Zealand Nissan Corporation and Financial Services ("Nissan") advises that its systems have been subject to a cyber incident. Nissan is working with its global incident response team and relevant stakeholders to investigate the extent of the incident and whether any personal information has been accessed. Nissan has also notified the Australian Cyber Security Centre and the New Zealand National Cyber Security Centre.

While the extent of the incident is still under investigation, Nissan encourages its customers to be vigilant across their accounts, including looking out for any unusual or scam activities. Nissan is working to restore its systems as soon as possible and will continue to provide updates by its website available via nissan.com.au and nissan.co.nz.

Nissan thanks you for your understanding during this process, and asks that you have patience with us and our staff while we do our best to work through these issues.

Some dealer systems will be impacted however, your local Nissan Dealership is operating. Please speak directly to your local Nissan dealer to assist with all vehicle and servicing queries.

FREQUENTLY ASKED QUESTIONS

WHAT HAS HAPPENED? +

The Australian and New Zealand Nissan Corporation and Financial Services ("Nissan Oceania") experienced a cyber incident on 5 December 2023 that impacted our IT servers in Australia and New Zealand.

We took immediate action to contain the breach, and alerted the relevant government authorities, including the Australian and New Zealand national cyber security centres and privacy regulators.

Since then, we have been working urgently with our global incident response team and external cyber forensic experts to review the compromised data and understand the impact on individuals within our community.

At this stage of our investigation, it has become clear that personal information belonging to some of Nissan's customers, dealers, and employees, has been compromised. This includes customers of our Mitsubishi, Renault, Skyline, Infiniti, LDV and RAM branded finance businesses.

WHAT INFORMATION WAS COMPROMISED? +

The type of information involved will be different for each person. Current estimates are that up to 10% of individuals have had some form of government identification compromised. The data set includes approximately 4,000 Medicare cards, 7,500 driver's licenses, 220 passports and 1,300 tax file numbers.

The remaining 90% of individuals being notified have had some other form of personal information impacted; including copies of loan-related transaction statements for loan accounts, employment or salary information or general information such as dates of birth.

HOW DO I KNOW IF MY DATA IS IMPACTED?

We are notifying affected individuals directly to tell them what information was involved, how we are supporting them, and the steps they can take to protect themselves.

We are committed to contacting affected individuals as soon as possible to tell them what information was involved, how we are supporting them, and the steps they can take to protect themselves against the risk of harm, identity theft, scams or fraud.

If you have not been contacted and you have any concerns about your data security, please contact **IDCARE**, the Australian and NZ national identity and cyber support service.

WHAT IS NISSAN DOING TO SUPPORT IMPACTED INDIVIDUALS?

There are several ways we are providing support and guidance for people who have been personally affected by this incident:

- We have already begun contacting people who have had sensitive information compromised to tell them what information was involved, what they need to do, and what support is available to them.
- **IDCARE:** We have partnered with IDCARE, Australia and New Zealand's national identity and cyber support community service. IDCARE's expert case managers will work with impacted individuals to address any concerns about risks to their personal information, and any instances where they think information might be misused. IDCARE's services are available at no cost to those affected by the cyber incident.
- **Equifax:** In Australia, we are providing free access to Equifax credit monitoring services for 12 months to watch for any fraudulent activity.
- **Centrix:** In New Zealand, we are providing customers with free access to Centrix to assist with the provision of a credit report and placement of a credit freeze on their credit file.
- **ID replacement:** Where someone's primary identity documents have been compromised, and the advice from the issuing government agency is to replace the document, Nissan will reimburse the cost of the replacement.
- **Customer support line:** We have established a dedicated customer support line which can be contacted between 7am and 7pm AEDT weekdays on:
  - **Australia** 1800 958 000
  - **New Zealand** 0800 44 50 14

WHAT CAN I DO?

We continue to encourage everyone to take the following steps to protect against identity theft, scams or fraud:

- Be vigilant for any unusual or suspicious online activity.
- Avoid clicking on any links or opening any suspicious emails or attachments.
- Be vigilant for any unrecognised or unsolicited telephone calls, emails or messages asking you to provide personal information.
- Always verify the sender of any communications received to make sure they're legitimate.
- Update your passwords regularly, using 'strong' passwords and not re-using passwords for multiple accounts.
- Enable multi-factor authentication for your online accounts where available.
- Contact IDCare, the Australian and NZ national identity and cyber support service.
- Report a scam in Australia by visiting Scamwatch at www.scamwatch.gov.au

- Request a free credit report from a credit reporting body, if you are in Australia (Equifax, illion and Experian), or from a credit reporting agency if you are in New Zealand (Centrix, Equifax and illion) and check for any applications or requests that you did not make.

ARE DEALERSHIPS IMPACTED? +

Your local Nissan dealership is operating. Please speak directly to your local Nissan dealer to assist with all vehicle and servicing queries.

HOW CAN I CONTACT NISSAN? +

We will continue to post updates here as they become available.

We have established a dedicated customer support line for individuals who have received an email or letter notification. They can be contacted between 7am and 7pm AEDT weekdays on:

- **Australia** 1800 958 000
- **New Zealand** 0800 44 50 14

BACK TO HOMEPAGE