Dear Nissan Employee:

We are writing to share an important message regarding employees' personal information. Nissan Americas uses Oracle PeopleSoft software to manage employee information, including payroll, tax administration, and other personnel records. Oracle has informed us that there was a cyber event and that the personnel records of hundreds of companies may have been obtained by so-called threat actors. We have since learned that Nissan was specifically targeted in this attack.

Upon learning about this issue, we quickly activated incident response protocols. We have been in communication with authorities throughout our response to this attack. Our technical teams, along with external experts, have secured our systems and will continue to work with Oracle to address this issue. We have taken steps designed to end unauthorized access and to prevent further disclosure of the information. We are also making arrangements for a free credit or dark web monitoring service offer to affected individuals where available.

We are working to complete our investigation as quickly as possible to understand the full scope and impact. Though we are early in that process, we believe some personal information has been accessed, such as contact and banking information, Social Security Number / Social Insurance Number / National Identification Number, financial and tax data, and dependent / beneficiary information. We believe that this incident affects current and former Nissan employees in the U.S.A., Canada, Mexico, and Brazil.

As we continue our investigation, individuals whose personal information has been exposed will receive further communication with additional details and next steps.

For now, you will be required to login through a network computer or a secured VPN connection to view pay slips or make direct deposit changes. If you need to make additional changes or obtain your paystub and you do not have access to an on-site computer or secured VPN connection, please open a case at Engage@Nissan. As a fraud protection measure, we are working to implement additional layers of identity authentication before processing payroll requests.

What you should do now: While we continue our investigation, we encourage all employees to take the following precautionary steps:

- **Remain vigilant** for suspicious emails, phone calls, or text messages requesting personal or company information. Do not click on unfamiliar links or attachments.
- **Change your passwords for all significant accounts (including your financial institutions)**, especially if you reuse passwords across personal or work accounts. Choose strong, unique passwords for each account.
- **Enable multi-factor authentication (MFA)** wherever available, particularly for personal banking, email, and financial accounts.

• **Monitor your financial accounts and credit reports for any unusual or unauthorized activity.** Report anything suspicious immediately to your financial institution. Reject any requests for bank details, access or identity confirmations that you receive through unusual means (mail, messaging, phone call).
• **Do not share any personal information (e.g., Social Security number, banking details)** unless you are certain of the request's legitimacy**.** Nissan will not ask for this information via unsolicited email, text, or phone call.

Additional information regarding this matter will come from official Nissan communications channels or your manager. If you receive suspicious communications via email, phone, or text, please report them immediately to infosec@nissan-usa.com.

The privacy and security of the personal information we maintain regarding our employees is of the utmost importance, and we are actively working through the situation. We will share updates and any actions required as soon as possible. We also will include information about additional support resources such as credit or dark web monitoring where available.

Thank you,

Leon Martinez
Vice President and Chief Human Resources Officer, Nissan Americas

_____

Employee Q&A

Q: What happened?
A: Oracle's PeopleSoft program – which manages employee records, payroll, and other personal data – experienced a cyber incident in which data was unlawfully accessed on Nissan's systems. We are actively investigating with internal teams and external experts to determine the nature and scope.

Q: What was the cybersecurity incident?
A: Cyber threats are an ongoing challenge across industries, and many recent incidents involve attacks on widely used systems and third-party platforms. In this instance, the attack involved an unknown vulnerability in Oracle's PeopleSoft software and is impacting hundreds of companies and institutions.

Q: What information may be involved?
A: Though we are early in the investigation, we believe that some personal employee information has been exposed, such as contact and banking information, Social Security Number / Social Insurance Number / National Identification Number, financial and tax data, and dependent / beneficiary information. We will provide specific details as they are confirmed.

Q: When did this occur?
A: We were recently made aware that Nissan was directly targeted in the cyber incident. Our teams acted immediately to confirm and contain the issue and begin remediation.

Q: How is the company addressing the incident?
A: We activated our incident response protocols right away. We have been in communication with authorities throughout our response to this attack. Our technical teams engaged cybersecurity experts, secured affected systems, and will continue to work with Oracle to address this issue. We have taken steps designed to end unauthorized access and to prevent further disclosure of the information. We are also making arrangements for a free credit or dark web monitoring service offer to affected individuals where available, and we are implementing additional layers of identity authentication before processing payroll requests.

Q: Can I still access HR payroll services?
A: At this time, you will be required to login through a network computer or a secured VPN connection to view pay slips or make direct deposit changes. If you need to make any additional changes or obtain your paystub and you do not have access to an on-site computer or secured VPN connection, please open a case at Engage@Nissan. As a fraud protection measure, we are working to implement additional layers of identity authentication before processing payroll requests.

Q: What should I do right now?
A:

- Be cautious of unsolicited emails, calls, or messages requesting personal information
- Change passwords for all significant accounts including your financial institutions (especially reused ones) and enable MFA where possible
- Monitor bank, credit, and other sensitive accounts for unusual activity
- Report suspicious communications on Nissan assets (email, phone, Teams chat, etc.) to *infosec@nissan-usa.com*.

Q: How will I know if my information was affected?
A: If the investigation determines that your specific information was involved, you will be notified with additional details and support resources.

Q: Should I share my personal information if someone contacts me about this?
A: No. Do not share any personal information in response to unsolicited requests. Nissan will not ask for personal details via email, text, or phone related to this incident.

Q: When will we receive another update?
A: We will continue to provide updates as we learn more. Our priority is to share accurate information as quickly as possible.

Q: Where can I go with questions?
A: We will continue to provide updates on the investigation and credit or dark web monitoring offer as we learn more. Our priority is to share accurate information as quickly as possible. If you do not have access to a network computer or VPN connection and you need to make any additional changes, require a paystub, or have any additional questions concerning payroll services, please open a case at Engage@Nissan.

###