BASS BERRY + SIMS

Kathryn Walker
kwalker@bassberry.com
(615) 742-7855

May 14, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Maryland Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: ***Nissan North America, Inc.: Notification of Data Incident***

Dear Attorney General Brown:

Pursuant to Md. Code Ann., Com. §§14-3501 – 14-3508, I am notifying you of a data security incident involving Maryland residents.

IDENTIFICATION OF PARTIES

This notice is provided by Bass Berry & Sims, PLC on behalf of Nissan North America, Inc. ("NNA"), located at One Nissan Way, Franklin, TN 37067. Bass Berry & Sims, PLC serves as counsel for NNA.

SYNOPSIS OF THE DATA SECURITY INCIDENT AND RESPONSE

On November 7, 2023, NNA learned it was the victim of a targeted attack against its external VPN when a criminal threat actor deliberately shut down certain NNA systems and demanded a ransom. Immediately upon discovering the criminal attack, NNA (working very closely with external cybersecurity professionals experienced in handling these types of complex security incidents) investigated, contained, and successfully terminated the threat. NNA promptly notified law enforcement of the data incident. On December 5, 2023, NNA notified all current employees of the incident, the possibility that certain employee personal information could have been accessed and that NNA would notify impacted individuals pending investigation.

Through its investigation, NNA learned the criminal threat actor accessed data from a number of NNA's local and network shares but did not encrypt any data or render any of NNA's systems inoperable. NNA conducted a thorough analysis of the potentially accessed data and throughout its forensic review found that nearly all implicated data was business information and did **not** contain Personal Information. However, on or about February 28, 2024, NNA identified certain Social Security Numbers in the data primarily relating to current and former NNA

employees residing in Maryland, as well as limited financial account information for one Maryland resident. At this time, NNA has no indication that any information has been misused or was the attack's intended target.

NUMBER OF MARYLAND RESIDENTS AFFECTED

At this time, NNA is aware of 158 Maryland residents affected by this incident. Pursuant to Md. Code Ann. Com. §§14-3501 – 14-3508, these residents are receiving written notice of the incident on 05/15/2024. NNA is also providing your office with a representative copy of the notice to affected residents with this submission.

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Since the attack, NNA has taken several steps to strengthen its security environment, including an enterprise-wide password reset, implementation of Carbon Black monitoring on all compatible systems, vulnerability scans, and other actions to address unauthorized access. NNA is currently reviewing its security processes and procedures for additional recommended remediation and protection efforts.

Although NNA is not aware of any instances of fraud or identity theft resulting from this incident, it is providing affected residents, at no charge, with access to Experian's IdentityWorks services for 24 months from the date of enrollment. NNA is also providing proactive fraud assistance to help with any questions that affected residents might have or in the event that they become a victim of fraud.

Please contact me should you need any additional information about the incident.

Sincerely,

/s/ Kathryn Walker

Kathryn Walker

NISSAN

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 15, 2024

L2231-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 EMPLOYEE
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

Please read this letter in its entirety.

The privacy and security of the personal information we maintain regarding our employees is of the utmost importance to Nissan North America, Inc. ("Nissan"). We're writing with important information regarding an incident that involved some of your personal information. This letter will provide you with relevant information about the incident, let you know about the significant measures we take to protect our employees' information, and explain the services we are providing to assist you and actions that you can take.

WHAT HAPPENED?

As shared during the Nissan Town Hall meeting on December 5, 2023, Nissan learned on November 7, 2023 that it was the victim of a targeted cyberattack. Upon learning of the attack, Nissan promptly notified law enforcement and began taking immediate actions to investigate, contain, and successfully terminate the threat. Nissan worked very closely with external cybersecurity professionals experienced in handling these types of complex security incidents. Nissan has been reviewing the compromised data and recently discovered files containing certain personal information of our employees. At this time, we have no indication that any information has been misused or was the intended target of the unauthorized actor.

WHAT INFORMATION WAS INVOLVED?

Through our investigation, Nissan recently learned that the unauthorized actor may have accessed, viewed, or removed documents with the following types of information about you: [data elements].

The data accessed did not include any of your Financial Information.

WHAT WE ARE DOING

Nissan values our employees' privacy and deeply regrets that this incident occurred. Nissan has made further enhancements to our systems, security, and practices. We have engaged appropriate cybersecurity experts to assist us in conducting a review of our security practices and systems to ensure that enhanced security protocols are in place going forward to reduce the risk of this type of incident occurring in the future.

Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are providing you, at no charge, with access to Experian's IdentityWorks services, which are explained below. This is in addition to the employee benefit you may have elected with Nissan. These complimentary credit services are being provided to you for 24 months from the date of enrollment. Finally,

Nissan is providing you with proactive fraud assistance to help with any questions you might have or if you become a victim of fraud. These services are provided by Experian, a company specializing in fraud assistance and remediation services.

WHAT YOU CAN DO

Again, we have no evidence that your personal information has been misused. However, to protect you from the potential misuse of your information, we encourage you to take advantage of the complimentary credit services offer included in this letter.

To help protect your identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **August 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-6266 by **August 30, 2024**. Be prepared to provide engagement number **B120412** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE**: You receive the same Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.[2]

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-6266. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additionally, we recommend that you remain vigilant to prevent identity theft and fraud by monitoring your credit reports and financial institution and other account statements. We also recommend that you promptly report any suspicious activity or suspected identity theft to law enforcement or your state's attorney general.

If you choose not to use the credit monitoring services described above, we encourage you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. Hearing-impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.

FOR MORE INFORMATION

We hope this information is helpful to you. If you have questions, representatives are available for 90 days from the date of this letter to assist you with enrolling in the complimentary credit monitoring services, between the hours of 9:00 a.m. to 9:00 p.m. Eastern, Monday through Friday, excluding holidays. Please call the dedicated, external help line at 833-931-6266 and be prepared to share your engagement number B120412.

Nissan values its employees and takes its responsibility to protect your personal information very seriously. We sincerely regret any inconvenience or concern this incident may cause and appreciate your continued efforts on behalf of Nissan.

Sincerely,

Leon Martinez
Vice President, Human Resources

William Orange
Vice President, IS/IT and Chief Information Officer

0000001

STATE NOTIFICATIONS

For Maryland residents: The Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD, 21202; www.marylandattorneygeneral.gov; 1-888-743-0023; consumer hotline (410) 528-8662.

For Massachusetts residents: It is required by state law that you are informed of your right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For New Mexico residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. It is important that you remain vigilant by reviewing all of your account statements and that you obtain a free copy of your credit report in order to monitor it for unauthorized changes.

For New York residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol Albany, NY 12224-0341, 1-800-771-7755 (toll-free), (800) 788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/. You can contact the Bureau of Internet and Technology (BIT) at: 28 Liberty Street, 15th Floor, New York, NY 10005, Phone: (212) 416-8433, https://ag.ny.gov/resources/individuals/consumer-issues/technology.

For North Carolina residents: You can obtain information from the Federal Trade Commission and the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.

For Oregon residents: We encourage you to report suspected identity theft to the Federal Trade Commission and the Oregon Attorney General. The Oregon Attorney General can be reached at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400 http://www.doj.state.or.us.

For Rhode Island residents: You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov.

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account. This incident affected 17 Rhode Island residents.

For Vermont residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's office at: 1-800-649-2424 (toll-free in Vermont); (802) 656-3183. This incident affected 3 Vermont consumers.

For Washington, D.C. residents: You may contact the Federal Trade Commission or the Office of the Attorney General for the District of Columbia to receive additional information about steps to take to avoid identity theft. The Office of the Attorney General can be reached at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; https://oag.dc.gov/; 1-202-727-3400.