

NH DEPT OF JUSTICE
FEB 9 '23 PM 12:13

February 3, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED**FEB 09 2023****Re: Notice of Data Event****CONSUMER PROTECTION**

Dear Ladies and Gentleman,

Bass, Berry & Sims PLC represents Nissan North America, Inc. ("Nissan"). I am writing to provide notification of an incident at a third-party service provider for Nissan, LumenData, Inc. ("LumenData") that involved the security of personal information of 20 New Hampshire residents. This notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Nissan does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

LumenData provides software development services to Nissan. Nissan provided certain information to LumenData for processing during the testing of the software. On June 21, 2022, Nissan received notice that certain data it provided for software testing had inadvertently been exposed by LumenData. During Nissan's investigation, on September 26, 2022, Nissan determined that this incident likely resulted in unauthorized access or acquisition of data, including some personal information belonging to Nissan customers. Specifically, the data embedded within the code during software testing was unintentionally and temporarily stored in a cloud-based public repository.

Upon learning of this issue, Nissan immediately ensured that LumenData contained the threat by disabling all unauthorized access to the data, and we commenced a prompt and thorough investigation. Nissan worked with LumenData to assure that it took steps to prevent events like this in the future. As part of the investigation, Nissan worked very closely with external cybersecurity professionals experienced in handling these types of complex security incidents. The information that was potentially accessed or acquired during the time that it was temporarily available on a public repository included each impacted New Hampshire resident's name, date of birth, and NMAC (Nissan Motor Acceptance Company) account number. This information did not include Social Security numbers, credit card information or access codes to NMAC accounts.

February 3, 2023

Page 2

Nissan is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Nissan wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud.

Notice to New Hampshire Residents

On or about December 19, 2022, Nissan provided the affected residents with written notification of this incident in substantially the same form as the letter attached hereto. Nissan is offering the affected residents complimentary one-year membership with a credit monitoring service. Nissan advised the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Nissan advised the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the New Hampshire Attorney General, and the Federal Trade Commission.

We can assure you that this incident was an isolated one, and we remain fully committed to maintaining the privacy of personal information in our possession or accessed by our vendors. Nissan continues to evaluate and modify our practices and procedures, including those required of third-party service providers, to enhance the security and privacy of personal information.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at

Sincerely,

Roy Wyman
Member

RHW:kd

Enclosures

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

NOTICE OF DATA BREACH

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

The privacy and security of the personal information we maintain is of the utmost importance to Nissan North America, Inc. ("Nissan"). We're writing with important information regarding a data security incident at a third-party service provider for Nissan that involved some of your information. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

The impacted third-party service provider provides software development services to Nissan. Nissan provided certain information to this service provider for processing during the testing of the software.

On June 21, 2022, Nissan received notice that certain data it provided for software testing had inadvertently been exposed by the third-party service provider. During our investigation, on September 26, 2022, we determined that this incident likely resulted in unauthorized access or acquisition of our data, including some personal information belonging to Nissan customers. Specifically, the data embedded within the code during software testing was unintentionally and temporarily stored in a cloud-based public repository.

What We Are Doing.

Upon learning of this issue, we immediately ensured that the third-party provider contained the threat by disabling all unauthorized access to the data, and we commenced a prompt and thorough investigation. We worked with the third-party service provider to assure that it takes steps to prevent events like this in the future. As part of our investigation, we worked very closely with external cybersecurity professionals experienced in handling these types of complex security incidents.

What Information Was Involved.

The information that was potentially accessed or acquired during the time that it was temporarily available on a public repository included your name, date of birth, and NMAC account number. This information did *not* include your Social Security number or credit card information.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this event occurred. We can assure you that this incident was an isolated one, and we remain fully committed to maintaining the privacy of personal information in our possession or accessed by our vendors. We will continue to evaluate and modify our practices and procedures, including those required of third-party service providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at . This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 am to 9:00 pm Eastern time.

Sincerely,

Nissan North America, Inc.

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. **ENROLL** by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. **VISIT** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. **PROVIDE** the Activation Code: <<Enrollment Code>>

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 877.288.8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT
3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance™:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877.288.8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

2. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
[https://www.equifax.com/personal/
credit-report-services/credit-fraud-alerts/](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
[https://www.experian.com/
fraud/center.html](https://www.experian.com/fraud/center.html)
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888) 298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Dear <<Name1>>:

The privacy and security of the personal information we maintain is of the utmost importance to Nissan North America, Inc. ("Nissan"). We're writing with important information regarding a data security incident at a third-party service provider for Nissan that involved some of your information. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

The impacted third-party service provider provides software development services to Nissan. Nissan provided certain information to this service provider for processing during the testing of the software.

On June 21, 2022, Nissan received notice that certain data it provided for software testing had inadvertently been exposed by the third-party service provider. During our investigation, on September 26, 2022, we determined that this incident likely resulted in unauthorized access or acquisition of our data, including some personal information belonging to Nissan customers. Specifically, the data embedded within the code during software testing was unintentionally and temporarily stored in a cloud-based public repository.

What We Are Doing.

Upon learning of this issue, we immediately ensured that the third-party provider contained the threat by disabling all unauthorized access to the data, and we commenced a prompt and thorough investigation. We worked with the third-party service provider to assure that it takes steps to prevent events like this in the future. As part of our investigation, we worked very closely with external cybersecurity professionals experienced in handling these types of complex security incidents.

What Information Was Involved.

The information that was potentially accessed or acquired during the time that it was temporarily available on a public repository included your name and date of birth. This information did *not* include your Social Security number or credit card information.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this event occurred. We can assure you that this incident was an isolated one, and we remain fully committed to maintaining the privacy of personal information in our possession or accessed by our vendors. We will continue to evaluate and modify our practices and procedures, including those required of third-party service providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at . This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 am to 9:00 pm Eastern time.

Sincerely,

Nissan North America, Inc.

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. **ENROLL** by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. **VISIT** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. **PROVIDE** the Activation Code: <<Enrollment Code>>

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 877.288.8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877.288.8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

2. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888) 298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.