



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

April 24, 2023

Bruce A. Radke
312-463-6211
312-819-1910
bradke@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Potential Data Security Incident

Dear Mr. Karberg:

We represent Napleton Automotive Group (“Napleton”), One Oakbrook Terrace, Suite 600, Oakbrook Terrace, IL 60181, in connection with an incident that may have involved the personal information of one (1) Maryland resident. Napleton is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Napleton is notifying you of this incident, Napleton does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

On February 13, 2023, Napleton learned of suspicious activity on its network. Upon discovering the incident, Napleton promptly began an internal investigation, notified law enforcement, and engaged a forensic security firm to investigate and secure its computer systems. The investigation determined that an unknown third party accessed Napleton’s systems from on or about February 7, 2023 to February 10, 2023, and that certain personal information may have been accessed and/or acquired from its system as a part of the incident. Napleton conducted a comprehensive review of the involved data to determine if it contained any personal information. On or about March 3, 2023, Napleton determined that the data contained the name, Social Security number, driver’s license/state identification number, and/or passport number of one (1) Maryland resident. At this point, Napleton is not aware of any fraud or identity theft to any individual as a result of this incident.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

April 24, 2023

Page 2

NOTICE TO MARYLAND RESIDENT

Napleton is notifying the one (1) Maryland resident of the incident by letter today, April 24, 2023. The notification letter will include an offer for twelve (12) months of complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the Maryland resident via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Napleton promptly prevented further unauthorized access to the system. It also notified law enforcement and engaged a forensic security firm to investigate and confirm the security of its computer systems. Napleton is undertaking efforts to reduce the risk of a similar incident occurring in the future, including enhancing its technical security measures. Finally, as discussed above, Napleton is notifying the potentially involved individuals, providing free credit monitoring services to the Maryland resident, and providing individuals with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,



Bruce A. Radke

Enclosure



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

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

<<Date>>

Dear <<Name 1>>:

Napleton Automotive Group (“Napleton”) values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On February 13, 2023, we discovered unusual activity on our computer network. Upon identifying the issue, we promptly began an internal investigation and began restoring our systems. We also notified law enforcement and engaged a forensic security firm to investigate and confirm the security of our computer systems. The forensic investigation recently concluded, and it determined that an unknown third party accessed our systems from on or about February 7, 2023 until February 10, 2023 and may have accessed and acquired certain documents from our systems as a part of the incident.

What Information Was Involved? Out of an abundance of caution, we are notifying all individuals we have been able to identify whose personal information may have been contained in the documents that may have been accessed. On or about March 3, 2023, we determined that those documents may have contained information that included your name, Social Security number, driver’s license/state identification number, and/or passport number.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft involving your information, we are also offering a complimentary one-year membership of Equifax Credit Watch™ Premier. 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. Equifax Credit Watch™ Premier is completely free to you. Enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Equifax Credit Watch™ Premier, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.**

What You Can Do. While we have no evidence that your personal information has been misused as a result of this incident, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call 866-516-8139 from 9 a.m. – 9 p.m. Eastern, Monday through Friday.

Sincerely,

Napleton Automotive Group



<<Name1>>
Enter your Activation Code: <<ACTIVATIONCODE>>
Enrollment Deadline: <<ENROLLMENTDEADLINE>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security number, credit/debit card, or bank account numbers are found on fraudulent internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out-of-pocket expenses resulting from identity theft⁶
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit, and personal identification cards

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATIONCODE>>, then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue.”
If you already have a myEquifax account, click the “Sign in here” link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click “Sign Me Up” to finish enrolling.
You’re done!
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the internet addresses of these suspected internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible internet site where consumers’ personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state, and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant, or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.