Clark Hill

Ilya A Smith
T (312) 985-5939
F (312) 517-7573
Email: jsmith@clarkhillcom

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

July 15, 2022

Via Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Aaron Frey:

We represent Central Maine Motors Auto Group ("CMMAG"), with respect to a security incident involving the possible exposure of certain personally identifiable information ("PII") described in more detail below. CMMAG is committed to answering any questions you may have about the security incident, its response, and steps taken to minimize the risk of a similar incident in the future.

1. Nature of security incident.

Earlier this year in January, an unencrypted thumb drive used to transfer files between computers was lost. CMMAG worked with legal counsel to investigate the loss and to determine what may have been present on the thumb drive. CMMAG was unable to determine with 100% certainty that there was no employee personal information present on the thumb drive. While CMMAG believes that is it very unlikely that the thumb drive contains employee personal information, out of an abundance of caution, CMMAG notified current and former employees about the incident. If current and former employee information was present on the thumb drive, this would include data elements such as names, Social Security numbers, dates of birth and dates of employment.

2. Number of residents affected.

This incident affected five hundred and sixty-nine (569) Maine residents. The impacted individuals were mailed a notification letter on July 15, 2022. A copy of the notification letter is attached as Exhibit A.

3. Steps taken relating to the incident.

Since the incident, CMMAG has taken steps to minimize the risk of this happening in the future. For example, CMMAG has implemented a new policy where only encrypted thumb drives may be used. Additionally, CMMAG is providing credit monitoring and identity protection services to all those impacted by the incident, at no cost for 24 months.

4. Contact information.

CMMAG takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at ismith@clarkhill.com or (313) 309-9466.

Very truly yours,

CLARK HILL

Ilya A Smith
Senior Counsel

(Enclosure)

cc: Melissa Ventrone, Clark Hill, PLC

Central Maine Motors Auto Group
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

July 15, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Central Maine Motors wants you to know about a data security incident that may have impacted some of your personal information, like your name, Social Security number, date of birth, and employment date. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps that you can take to protect your personal information and the resources we are making available to help you.

What happened?

Earlier this year in January, we learned that a thumb drive used to transfer files between computers was lost. We investigated the loss and it took some time to determine what may have been present on the thumb drive. While we think the probability is very low, in our investigation we recently determined that the thumb drive may have been used to transfer one or two files containing employee information. We wanted to let you know about this incident out of an abundance of caution because we are not able to determine, with 100% certainty, that your information was not present on the thumb drive.

What information was involved?

Information that may have been present on the thumb drive includes your name, Social Security number, date of birth and employment dates.

What we are doing:

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since this incident we have put in place a policy preventing the use of unencrypted thumb drives for personal information, like HR files. Further, we are conducting a comprehensive review of our security processes and systems.

In addition, we are offering, at no cost, identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What you can do:

You should remain vigilant for incidents of identity theft or fraud for the next 12 to 24 months. It is always a good idea to review your bank account and other financial statements as well as your credit reports for suspicious activity.

We also encourage you to contact IDX with any questions and to take full advantage of the IDX service offerings. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 15, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

If you wish to enroll in the monitoring services, but do not have a computer available to you from which you can complete this enrollment, Central Maine Motors will have a computer available to you from which you can complete the enrollment process.

For more information

For more information about this incident, please call 1-800-939-4170 between the hours of 9 am - 9 pm Eastern Time, Monday through Friday. The privacy and security of your information is of the upmost importance to us, and we sincerely apologize for any inconvenience this may cause you.

Sincerely,

Chris Gaunce, President

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code referenced above.

2. Activate the credit monitoring provided as part of your services with IDX. The monitoring included must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to provide guidance.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX credit monitoring, notify them immediately by calling 1-800-939-4170 from 9 am - 9 pm Eastern Time, Monday through Friday.

A representative will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be able to work with a representative who will assist you with resolving any fraudulent activity.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.