Clark Hill

RECEIVED

OCT 22 2025

CONSUMER PROTECTION

Jason M. Schwent
T (312) 985-5939
Email: jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

October 16, 2025

VIA POSTAL MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Formella:

We represent Copeland Auto Group ("Copeland") with respect to a data security incident involving personal information as described below. Copeland takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On September 2, 2025, Copeland identified suspicious activity within an email account on its systems. Copeland immediately secured its email environment, changed the password associated with the impacted email account, and engaged independent computer forensic experts to assist. The investigation determined that one (1) employee email account was compromised for a limited period of time. Copeland reviewed the contents of the email account and determined that personal information was in the account.

Impacted information includes names, Social Security numbers, driver's license numbers, state ID numbers, passport numbers, payment card information, financial account information, and health information.

2. Number of New Hampshire residents affected

One (1) resident of New Hampshire was notified of the incident. Notification letters were sent to potentially affected individuals on October 16, 2025. A copy of the notification letter is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, Copeland changed the password to the email account, ensured multi-factor authentication is implemented throughout the email environment, and installed new threat detection and log monitoring software on the email tenant, among other measures. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through Kroll.

4. Contact information

Copeland takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Member

cc: Sunaina Ramesh – sramesh@clarkhill.com

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

<<B2B_TEXT_1(NOTICE OF DATA SECURITY INCIDENT/BREACH)>>

Dear <<First_Name>> <<Last_Name>>,

Copeland Auto Group ("Copeland") recently experienced a data security incident that may have impacted some of your personal information. Copeland may have your information if you are currently or were previously a customer of Copeland. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you.

What Happened?

On September 2, 2025, we identified suspicious activity within an email account on our systems. We immediately secured our email environment, changed the password associated with the impacted email account, and engaged independent computer forensic experts to assist us in investigating what happened and what information may have been impacted. The investigation determined that one (1) employee email account was compromised for a limited period of time. We reviewed the contents of that email account and determined that personal information associated with you was in that account during the unauthorized access. Although we have no evidence that your personal information was misused, we are providing this notice out of an abundance of caution.

What Information Was Involved?

From our review, it appears that an email or attachment in the email account during the time of compromise contained your <<b2b_text_2 (data elements)>>.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have changed the password to the email account, and ensured multi-factor authentication is implemented throughout our email environment, among other measures. In addition, although there has been no evidence that your information was misused, we are offering <<ServiceTerminMonths>> months of complimentary identity monitoring services through Kroll.

What You Can Do:

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: `<<Membership Number (S_N)>>`

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. 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.

For More Information:

If you have questions, please call [redacted] between 9:00 a.m. – 6:30 p.m. Eastern Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

Copeland Auto Group

Recommended Steps to help Protect your Information

1. Website and Enrollment.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: `<<Membership Number (S_N)>>`

2. 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.

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.

3. 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 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 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.

4. 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.

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

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.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/201504_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. <<b2b_text_3(A total of [Number] Rhode Island residents were notified of 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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.