MORRISON FOERSTER

250 WEST 55TH STREET
NEW YORK
NEW YORK 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

AMSTERDAM, AUSTIN, BERLIN, BOSTON, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, MIAMI, NEW YORK, PALO ALTO, SAN DIEGO, SAN FRANCISCO, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

November 3, 2025

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

To Whom It May Concern:

On behalf of our client, Hyundai AutoEver America, LLC ("HAEA" or "the company"), a technology services provider which supports Hyundai's automotive operations in the United States, I am writing to notify you of a cyber incident potentially involving the personal information of Maine residents.

As background, on or around March 1, 2025, HAEA became aware of a cyber incident that impacted the company's information technology environment. Upon discovery, the company immediately launched an investigation with the support of external cybersecurity experts to assess the scope of the incident, confirm containment, and identify any affected information. HAEA also coordinated its efforts with law enforcement.

Through its investigation, the company determined that unauthorized activity began on February 22, 2025, and the last observed unauthorized activity occurred on March 2, 2025. During this period, an unauthorized third party had access to certain personal information stored on affected systems, including information associated with Maine residents. More specifically, HAEA determined that the affected data included individuals' names and Social Security numbers. Due to the nature of the incident, HAEA attempted to determine whether threat actors acquired the information at issue, which it could not fully confirm. Nevertheless, HAEA decided, in an abundance of caution, to provide the notification referenced below.

On October 30, 2025, HAEA mailed individual notification letters to 1 Maine resident. HAEA offered impacted individuals 24 months of complimentary identity protection services through Epiq Privacy Solutions, which include, among other things, three-bureau credit monitoring and identity protection services. Attached is a sample of the letter HAEA sent to Maine residents.

In response to this incident, HAEA terminated the unauthorized third party's access to the affected portion of its environment. The company engaged third-party forensic experts to assist with the investigation and response and has taken steps to implement additional security enhancements designed to reduce future risk, including blocking known indicators of compromise and strengthening its security monitoring and logging capabilities.

If you have any questions, please do not hesitate to contact me at +1 (213) 892-5268, by mail at 707 Wilshire Boulevard, Suite 6000, Los Angeles, CA 90017, or by email at EChang@mofo.com.

Sincerely,

Edward Chang
Partner | Morrison & Foerster LLP

HYUNDAI AutoEver

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

<<Date>>

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

Notice of Data Breach

Dear <<First Name>>,

On behalf of Hyundai AutoEver America, LLC ("HAEA," "we," or "us"), we are writing to inform you about an incident that may have involved personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. On March 1, 2025, HAEA became aware of a cyber incident that impacted our information technology environment. Upon discovery, we immediately launched an investigation with the support of external cybersecurity experts to assess the scope of the incident, confirm containment, and identify any affected information. HAEA also worked with law enforcement. Through our investigation, we determined that the unauthorized activity appears to have begun on February 22, 2025, and the last observed unauthorized activity occurred on March 2, 2025.

WHAT INFORMATION WAS INVOLVED. Based on our analysis to date, we have determined that the information about you that may have been affected in this incident included your name, <<Data Elements>>.

WHAT WE ARE DOING. We began investigating the incident as soon as we learned of it. After becoming aware of the incident, we immediately took steps to terminate the unauthorized third party's access to the affected portion of our environment. We engaged third-party cybersecurity specialists to assist with the investigation and response. The nature and scope of the incident required us to spend significant time and resources to analyze the available data and forensic information to complete our investigation. We continue to invest in additional security enhancements designed to mitigate future risk.

WHAT YOU CAN DO. We are providing you with the enclosed information about steps that you can take to protect against potential misuse of personal information to the extent it was obtained by the unauthorized third party. Additionally, as a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year credit monitoring service. We have engaged Epiq to provide you with its Epiq Privacy Solutions, which include, among other things, three-bureau credit monitoring and identity protection services. You have 90 days from the date of this letter to activate this free credit monitoring service by using the following enrollment code: <<Activation Code>>. This code is unique for your use and should not be shared. To enroll, go to www.privacysolutionsid.com or call 866-675-2006.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. If you have any questions or concerns, please do not hesitate to contact us at 855-720-3727.

Sincerely,

Hyundai AutoEver America, LLC

Steps You Can Take to Protect Against Potential Misuse of Personal Information:

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("**FTC**") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, at www.ftc.gov/idtheft/, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you identify information on your credit report resulting from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022
www.TransUnion.com

You also have other rights under the Fair Credit Reporting Act ("**FCRA**"). For further information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to obtain credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it is required to notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth, and Social Security number. The credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

Office of the Attorney General
400 6th Street, NW Washington,
DC 20001
(202) 727-3400
https://oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft.

Office of the Attorney General of Iowa Consumer
Protection Division
Hoover State Office Building 1305
E. Walnut Street
Des Moines, IA 50319
(515) 281-5926
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
https://www.marylandattorneygeneral.gov/

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

North Carolina Department of Justice Attorney
General Jeff Jackson
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

IF YOU ARE A RHODE ISLAND RESIDENT: We have determined that the incident involved <<RI Count>> Rhode Island residents. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/