Scott Murphy
Special Counsel
scott.murphy@dentons.com
D +1 515 246 7809

Dentons Davis Brown PC
Dentons Tower
215 10th Street, Suite 1300
Des Moines, IA 50309
United States
dentons.com

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut St
Des Moines, Iowa 50319

By E-mail Only to: consumer@ag.iowa.gov

Re: Notice of Data Security Breach
Pursuant to Iowa Code § 715C.2

June 2, 2026

To Whom It May Concern:

This firm represents Karl Auto Group, 1101 SE Oralabor Rd, Ankeny, Iowa 50021 ("Karl Chevrolet" or the "Company") and is providing notice of a security breach affecting the personal information of Iowa consumers, as required by Iowa Code § 715C.2(8). This notice is being provided within five (5) business days of the Company's notification to affected consumers.

Description of the Breach
Karl Chevrolet recently became aware that an unauthorized third party gained access to certain computer systems used in the Company's business operations. The Company immediately engaged a third-party forensic cybersecurity firm to investigate the incident. The Company also notified the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC). The incident was reported to the FTC in connection with the Company's obligations under the FTC's Standards for Safeguarding Customer Information Rule (the "Safeguards Rule"), 16 C.F.R. Part 314, as the Company is a motor vehicle dealer (financial institution) subject to the Safeguards Rule.

Approximate Date of the Breach
Based on the forensic investigation conducted to date, the unauthorized access is believed to have occurred prior to March 27, 2026. The forensic investigation has not been able to determine a precise date of initial access, and the investigation is ongoing. However, the Company was alerted to the security breach on April 4, 2026.

Type of Personal Information Involved
The forensic investigation has confirmed that the types of personal information that may have been compromised include one or more of the following:

- Full name in combination with Social Security number
- Full name in combination with driver's license number or other government-issued identification number
- Full name in combination with financial account information
- Full name in combination with passport number and/or passport image

These categories of personal information constitute "personal information" as defined by Iowa Code § 715C.1(11).

Puyat Jacinto & Santos ► Link Legal ► Zaanouni Law Firm & Associates ► LuatViet ► For more information on the firms that have come together to form Dentons, go to dentons.com/legacyfirms

Number of Iowa Residents Affected
Based on the information available to date, the Company believes that the security breach affects more than five hundred (500) Iowa residents. The exact number of affected individuals has not yet been determined due to forensic limitations, including encrypted exfiltration channels that prevent full reconstruction of the scope of data accessed. The Company is continuing its investigation to determine the full scope of affected individuals.

Consumer Notification
The Company is notifying affected consumers by mail or email based on available contact information we have for those consumers. In addition, and out of an abundance of caution due to having insufficient contact information for some potentially affected consumers, the Company is also providing notice on its website and to statewide media. Such notifications occurred on or about June 2, 2026. The notification to consumers includes a description of the breach, the approximate date of the breach, the types of personal information involved, contact information for the three major credit reporting agencies, and advice to report suspected identity theft to local law enforcement or the Iowa Attorney General, as required by Iowa Code § 715C.2(5). A copy of the notification for affected consumers is included with this filing as "Exhibit A".

Remedial Actions
The Company has taken the following steps in response to the incident:
- Engaged a third-party forensic cybersecurity firm to investigate the breach and determine its scope. This investigation is ongoing.
- Reported the incident to the FBI and the FTC.
- Implemented enhanced security measures to help prevent a similar incident in the future.
- Engaged dark web monitoring services to monitor for potential misuse of the compromised personal information. To date, no evidence of misuse has been identified.

Ongoing Investigation
The forensic investigation is ongoing. Certain forensic limitations, including the inability to reconstruct the full content of exfiltrated data and limited log retention in certain environments, have prevented the Company from fully determining the scope of the breach. The Company will supplement this notice if the investigation reveals materially new information regarding the type of personal information compromised or the number of Iowa residents affected.

Contact Information
Should you require any additional information regarding this matter, please do not hesitate to contact the undersigned.

Sincerely,

Scott M. Murphy

Scott Murphy
Special Counsel
Dentons Davis Brown PC

EXHIBIT A

Karl Auto Group
<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

NOTICE OF DATA SECURITY INCIDENT

June 2, 2026
We are writing to inform you of an incident that may affect the security of certain personal information associated with your relationship with Karl Auto Group. We take the protection of your personal information seriously and are providing this notice to explain the incident, the steps we have taken in response, and the steps you can take to help protect yourself.

What Happened
Karl Auto Group recently became aware that an unauthorized third party gained access to certain computer systems used in our business operations. Upon discovering the incident, we immediately began an investigation with the assistance of a third-party forensic cybersecurity firm and we also notified the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC). The investigation is ongoing, and we are working diligently to determine the full scope of the incident.

Based on the investigation to date, we believe the unauthorized access occurred prior to March 27, 2026, but we did not become aware of it until April 4, 2026. During this period, the unauthorized third party may have accessed files and data stored on our computer systems that contained personal information belonging to current and former customers, employees, and other individuals who provided personal information to Karl Auto Group in the ordinary course of business.

What Information Was Involved
While the investigation is ongoing and the full scope of affected data has not yet been determined, we have confirmed that the types of personal information that may have been accessed include one or more of the following, depending on the individual:

- Full name
- Social Security number

- Driver's license number or other government-issued identification number
- Financial account information
- Passport number and/or passport image

Not all these data elements were necessarily affected for every individual. We are providing this notice to you because your personal information may have been stored on the systems that were subject to unauthorized access, and we were unable to rule out that your information was affected.

What We Are Doing
Upon discovering the incident, we took immediate steps to contain and remediate the threat, including engaging a third-party forensic cybersecurity firm to investigate. We have implemented additional security measures to help prevent a similar incident from occurring in the future. We also notified the FBI, the FTC, and the Iowa Attorney General.
We continue to evaluate and enhance our security practices. We have also engaged dark web monitoring services to monitor for any indication that the affected personal information is being misused. To date, no evidence of misuse of the personal information involved in this incident has been identified, but we will continue to monitor the situation.

What You Can Do
We recommend that you take the following steps to help protect your personal information:

Monitor your financial accounts and credit reports. Review your account statements, explanation of benefits statements, and credit reports carefully and regularly for any unauthorized activity. Under federal law, you are entitled to one free credit report every twelve months from each of the three major credit reporting agencies. To obtain a free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. You may also contact the three major credit reporting agencies directly:

- **Equifax** — P.O. Box 740241, Atlanta, GA 30374-0241 | 1-800-685-1111 | www.equifax.com
- **Experian** — P.O. Box 2002, Allen, TX 75013 | 1-888-397-3742 | www.experian.com
- **TransUnion** — P.O. Box 1000, Chester, PA 19016 | 1-800-916-8800 | www.transunion.com

Consider placing a fraud alert on your credit file. A fraud alert tells creditors to take extra steps to verify your identity before granting credit in your name. You may place an initial fraud alert, free of charge, with any one of the three major credit reporting agencies listed above, and that agency is required to notify the other two.

Consider placing a credit freeze (security freeze) on your credit file. A credit freeze restricts access to your credit report, making it more difficult for identity thieves to open new accounts in your name. You may place a credit freeze by contacting each of the three major credit reporting agencies listed above. There is no charge to place, temporarily lift, or permanently remove a credit freeze.

If your Social Security number may have been affected, we recommend that you consider contacting the Social Security Administration at 1-800-772-1213 or at www.ssa.gov to learn more about how to monitor and protect your Social Security number.

If your passport number or passport image may have been affected, we recommend that you contact the U.S. Department of State regarding passport reissuance, as valid passport numbers present an ongoing fraud risk until the document is replaced. You may contact the Department of State at 1-877-487-2778 or at travel.state.gov.

Report suspected identity theft. If you suspect that you are a victim of identity theft, you are advised to report the incident to your local law enforcement agency or to the Iowa Attorney General's Office. You may contact the Iowa Attorney General's Office at:

- **Office of the Attorney General of Iowa, Consumer Protection Division**
- Hoover State Office Building
- 1305 E. Walnut Street
- Des Moines, Iowa 50319
- Telephone: 1-515-281-5926 or 1-888-777-4590
- Website: www.iowaattorneygeneral.gov

You may also file a complaint with the Federal Trade Commission at www.identitytheft.gov or by calling 1-877-438-4338.

For More Information
We understand that this incident may cause concern, and we sincerely apologize for any inconvenience. If you have any questions or would like additional information, please contact us at 1-855-743-5185. Representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Sincerely,

Bret Moyer,
1101 SE Oralabor Rd, Ankeny IA 50021