

June 10, 2021

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Hoover State Office Bldg.
1305 E. Walnut
Des Moines, IA 50319

To whom it may concern,

We are writing on behalf of our client Volkswagen Group of America, Inc., including its operating divisions, Audi of America and Volkswagen of America (together “VWGoA”) regarding a security incident that affects residents of your state.

On March 10, 2021, VWGoA was alerted that an unauthorized third party may have obtained certain customer information. VWGoA immediately commenced an investigation to determine the nature and scope of this event. VWGoA also contacted federal law enforcement and retained outside data analytics and cybersecurity consultants. The investigation confirmed in early May 2021 that a third party obtained limited personal information received from or about United States and Canadian customers and interested buyers from a vendor used by Audi, Volkswagen, and some authorized dealers. This included information gathered for sales and marketing purposes from 2014 to 2019. VWGoA believes the data was obtained when the vendor left electronic data unsecured at some point between August 2019 and May 2021, when VWGoA identified the source of the incident. VWGoA discovered the information at issue included more sensitive personal information on or about May 24, 2021. VWGoA completed the analysis to identify which specific individuals were impacted on or about June 7, 2021.

This incident involves over 3.3 million individuals. For over 97% of the individuals, the exposed information consists solely of contact and vehicle information relating to Audi customers and interested buyers, including some or all of the following contact information: first and last name, personal or business mailing address, email address, or phone number. In some instances, the data also includes information about a vehicle purchased, leased, or inquired about, such as the Vehicle Identification Number (VIN), make, model, year, color, and trim packages.

For approximately 90,000 Audi customers or interested buyers, the data also includes more sensitive information relating to eligibility for a purchase, loan, or lease. Nearly all of the more

45 Offices in 20 Countries

Squire Patton Boggs (US) LLP is part of the international legal practice Squire Patton Boggs, which operates worldwide through a number of separate legal entities.

Please visit squirepattonboggs.com for more information.

010-9222-4139/1/AMERICAS

sensitive data (over 95%) consists of driver's license numbers. A very small number of records include data such as dates of birth, Social Security or social insurance numbers, account or loan numbers, and tax identification numbers. VWGoA has retained IDX to offer free credit protection services to these approximately 90,000 individuals, which includes the following services for individuals who choose to enroll: twenty-four (24) months of triple bureau credit monitoring services, \$1 million of insurance, and assistance in the event of identity theft.

Based on VWGoA's investigation to date, the number of individuals impacted in your state is:

Number of individuals with only contact and vehicle information impacted: 9,807

Number of individuals with more sensitive personal information impacted: 146

Please note, VWGoA is verifying addresses against the National Change of Address database so these numbers may change slightly.

VWGoA will begin notifying affected individuals on June 11, 2021, regardless of the sensitivity of the data, and will include reminders to remain alert for suspicious emails or other communications. Individuals will receive one of the two sample letters attached from either Audi of America or Volkswagen of America. VWGoA will direct one letter toward individuals whose contact and vehicle information was impacted, and the other toward individuals whose more sensitive information was also impacted. VWGoA is also notifying the three major credit reporting agencies.

Protecting the security of personal information is of the utmost importance to VWGoA and VWGoA sincerely regrets any inconvenience this incident has caused. VWGoA is conducting a full security review with the vendor to identify if further security enhancements are reasonable and appropriate.

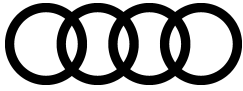
If you have any questions, please feel free to contact me at +1 202.457.6407 or elliott.golding@squirepb.com.

Sincerely,

Squire Patton Boggs (US) LLP



Elliot R. Golding



C/O IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 406-2408
Or Visit:
<https://response.idx.us/audivwdataprotect>
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

June 11, 2021

Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

What happened?

On March 10, 2021, we were alerted that an unauthorized third party may have obtained certain customer information. We immediately commenced an investigation to determine the nature and scope of this event. The investigation confirmed that the third party obtained limited personal information received from or about customers and interested buyers, including you, from a vendor used by Audi, Volkswagen, and some authorized dealers in the United States and Canada. This included information gathered for sales and marketing purposes from 2014 to 2019. We believe the data was obtained when the vendor left electronic data unsecured at some point between August 2019 and May 2021, when we identified the source of the incident.

On May 24, 2021, we confirmed that sensitive personal information was included in this incident.

What information was included?

The data included some or all of the following contact information about you: first and last name, personal or business mailing address, email address, or phone number. In some instances, the data also included information about a vehicle purchased, leased, or inquired about, such as the Vehicle Identification Number (VIN), make, model, year, color, and trim packages.

The data also included more sensitive information relating to eligibility for a purchase, loan, or lease. More than 95% of the sensitive data included was driver's license numbers. There were also a very small number of dates of birth, Social Security or social insurance numbers, account or loan numbers, and tax identification numbers.

What are we doing?

We take the safeguarding of your information very seriously. We have informed the appropriate authorities, including law enforcement and regulators. We are working with external cybersecurity experts to assess and respond to this situation and have taken steps to address the matter with the vendor.

As a result of this incident, we have partnered with IDX to provide you this notification and to offer you free credit protection services. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services should that occur. If you enroll in this protection, IDX will help you resolve issues if they arise.

What can you do?

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 406-2408 or going to <https://response.idx.us/audivwdataprotect> 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 September 11, 2021. We encourage you to take full advantage of this service offering.

As contact information was involved, please remain alert for suspicious emails or other communications that might ask for more information about you or your vehicle (commonly known as “phishing”). In particular:

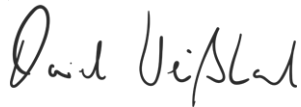
- Look out for spam emails or other communications requesting sensitive personal information. **We will never request sensitive personal information (such as credit card numbers, Social Security numbers, or passwords) through email or telephone communications.**
- Be cautious when opening links or attachments from unsolicited third parties. Unsolicited emails could contain computer viruses or other types of computer malware.

For more information:

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 406-2408 Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://response.idx.us/audivwdataprotect> for assistance or for any additional questions you may have.

Sincerely,



Daniel Weissland
President
Audi of America

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://response.idx.us/audivwdataprotect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership 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 assist you.

3. Telephone. Contact IDX at (833) 406-2408 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 identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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
1-800-525-6285
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 19016-2000
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.

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.

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

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.



C/O IDX
P.O Box 989728
West Sacramento, CA 95798-9728

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

June 14, 2021

Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

What happened?

On March 10, 2021, we were alerted that an unauthorized third party may have obtained certain customer information. We immediately commenced an investigation to determine the nature and scope of this event. The investigation confirmed that the third party obtained limited personal information received from or about customers and interested buyers from a vendor used by Audi, Volkswagen, and some authorized dealers in the United States and Canada. This included information gathered for sales and marketing purposes from 2014 to 2019. We believe the data was obtained when the vendor left electronic data unsecured at some point between August 2019 and May 2021, when we identified the source of the incident.

We have confirmed that your personal information was included in this incident.

What information was included?

The data included some or all of the following contact information about you: first and last name, personal or business mailing address, email address, or phone number. In some instances, the data also included information about a vehicle purchased, leased, or inquired about, such as the Vehicle Identification Number (VIN), make, model, year, color, and trim packages.

What are we doing?

We take the safeguarding of your information very seriously. We have informed the appropriate authorities, including law enforcement and regulators. We are working with external cybersecurity experts to assess and respond to this situation and have taken steps to address the matter with the vendor. As a result of this incident, we have also partnered with IDX to provide you this notification.

What can you do?

As contact information was involved, please remain alert for suspicious emails or other communications that might ask for more information about you or your vehicle (commonly known as “phishing”). In particular:

- Look out for spam emails or other communications requesting sensitive personal information. **We will never request sensitive personal information (such as credit card numbers, Social Security numbers, or passwords) through email or telephone communications.**
- Be cautious when opening links or attachments from unsolicited third parties. Unsolicited emails could contain computer viruses or other types of computer malware.

For more information:

Please call (833) 406-2408 Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://response.idx.us/audivwdataprotect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink that reads "Daniel Weissland". The signature is written in a cursive style with a large, looped 'D' at the beginning.

Daniel Weissland
President
Audi of America