



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>>

20575

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

June 11, 2021

### Notice of Data Breach

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

#### What happened?

We are writing to inform you of an incident that may have affected the security of your personal information.

**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:

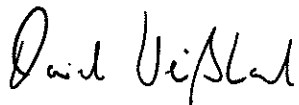
- Look out for spam emails or other communications requesting sensitive personal information. **We will never request sensitive personal information (such as credit card numbers, Social Security numbers, or passwords) through email or telephone communications.**
- Be cautious when opening links or attachments 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/auditwdataprotect> 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](http://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.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You should also know that if you are the victim of identity theft you have the right to file a police report if you ever experience identity fraud and obtain a copy of it. 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](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19016-2000  
[www.transunion.com](http://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.** You may place a freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. 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. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, to get a new credit card, employment, housing or other services until you temporarily lift or permanently remove the freeze. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies:

Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

**Equifax Security Freeze**

P.O. Box 105788

Atlanta, GA 30348

1-800-349-9960

<https://www.equifax.com/personal/credit-report-services/>

**Experian Security Freeze**

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

<https://www.experian.com/freeze/center.html>

**TransUnion Security Freeze**

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

<https://www.transunion.com/credit-freeze>

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

**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.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://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?

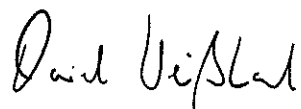
As contact information was involved, please remain alert for suspicious emails or other communications that might ask for more information about you or your vehicle (commonly known as “phishing”). In particular:

- 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 initial 'D'.

Daniel Weissland  
President  
Audi of America