

From:
To:
Subject: Notice of Data Security Incident
Date:

Dear StreetFire user:

We are writing to let you know that we recently discovered that some archived data from the prior streetfire.net website was acquired by an unauthorized party, including some of your information. Please review the information below.

What Happened?

On June 19, 2021, an unknown actor used what is believed to be a previously unknown technique to gain access to servers storing backup information regarding the prior streetfire.net website. Quickly after detecting the attack we took steps to remediate it, but the attacker was able to download certain files before being expelled.

What Information Was Involved?

We promptly retained leading cyber forensics firms to investigate the incident and conduct a thorough analysis of the files taken by the attacker. We learned July 16, 2021 that the information involved included information about your account and participation on the StreetFire site including your [REDACTED]

What Are We Doing?

After remediating the attack, we took steps to understand the nature and scope of the potential unauthorized access and engaged outside cybersecurity experts to investigate. We are working with these experts to assess the need for additional security measures, and we will continue to closely monitor our systems for unauthorized activity.

As an additional measure, we are offering you the option to enroll in one year of identity monitoring services from Identity Theft Guard Solutions (IDX). These services include CyberScan monitoring. If you would like to activate this coverage, please visit [REDACTED] and use the Enrollment Code below. IDX representatives are available Monday through Friday from 6 am to 6 pm Pacific Time. Please note the deadline to enroll is October 30, 2021.

Enrollment Code: [REDACTED]

What Can Happen Next and What Can You Do?

Because your information was exposed as a result of the attack, it is possible that unauthorized third parties try to use your information. We therefore recommend that you take extra precautions to protect yourself:

Although the StreetFire website is no longer active, we recommend that you change your password on any other service on which you use the same password you most recently used on streetfire.net.

You may also receive phishing emails to the email account you used to register your account at StreetFire (the email to which we are sending this notice), so you should exercise care when receiving unexpected emails.

This incident did not affect your credit or involve information used to obtain credit. However, we are required by law to provide additional information to you in this letter regarding those

issues. This information is provided below.

More Information

For the latest information on this incident you may contact us at privacy@motortrend.com or

On behalf of MotorTrend, we regret any inconvenience this may cause you.

Sincerely,

The MotorTrend Team

Identity Theft Information

This incident did not affect your credit or involve information that can be used to obtain credit. However, the following resources can help you learn more about protecting yourself or recovering from identity theft.

You have the right to put a fraud alert or security freeze on your credit report. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three credit reporting agencies will place an alert on your file at all three of them. A security freeze restricts all creditor access to your account, but might also delay any requests you might make for new accounts. Credit reporting agencies cannot charge you to place a security freeze.

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

You will need to supply your name, address, date of birth, Social Security number, and other personal information. The agencies are not permitted to charge you for placing or lifting a freeze. Each credit reporting agency will confirm your request with a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

Suspected identity theft should be reported to law enforcement, your attorney general, or the Federal Trade Commission, which also offers information about and responded to identity theft at IdentityTheft.gov. The FTC can be reached at:

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20850
1-877-ID-THEFT (1-877-438-4338)

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection. This office can be reached at:

New York State Division of Consumer Protection
123 William Street

One Commerce Plaza

New York, NY 10038-3804
1 (800) 697-1220
<http://www.dos.ny.gov/consumerprotection>

99 Washington Ave.
Albany, NY 12231-0001

IF YOU ARE A RHODE ISLAND RESIDENT: This incident affected an unknown number of Rhode Island residents. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

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

This email was sent by: IDX to michael.thomas@idx.us
10300 SW Greenburg Road Suite 570, Portland, OR, 97223 US
Privacy Policy
Click here to [unsubscribe](#)