April 14, 2023

VIA EMAIL

Consumer Protection & Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Breach, Confidential & Exempt from Public Records Act.

To Whom It May Concern:

We represent Hoosier Racing Tire Corporation ("Hoosier") and are notifying your office with respect to a data security event involving certain personal information of New Hampshire residents. By providing this notice, Hoosier does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Security Incident

Hoosier hired third-party vendors to build and operate its ecommerce website, including where payment card information was collected. Hoosier learned that unauthorized code was installed on this vendor-managed site between November 2020 and September 2022. This code may have captured personal information from residents of your state, including when the resident made a purchase on the website during this time period.

Hoosier learned through an email notification from its payment card service provider that its website contained an unauthorized Google Tag Manager script that could be acquiring user , including . Upon learning of this, Hoosier immediately contacted its website provider. A preliminary investigation was conducted by the third-party responsible for operation of Hoosier's website but the investigation was inconclusive as to whether personally identifiable information was actually acquired by the script.

Subsequently, a leading forensic investigating firm was engaged by counsel to investigate the script and the website. This forensic firm confirmed on March 9, 2023, that and other personal information was likely acquired by this Google Tag Manager script. The forensic firm determined that the

web transactions through the website were at risk of unauthorized acquisition between November 26, 2020, and September 16, 2022.

Steps Taken in Response to the Security Incident

Hoosier took immediate steps once it was notified of the unauthorized script and the unauthorized script was taken off of the website promptly. Hoosier has also switched website providers and has stopped using the technology that was vulnerable to the script.

Hoosier sent notification letters to the affected New Hampshire residents on April 14, 2023, via regular U.S. mail. A copy of the template notification letter is enclosed. In addition, Hoosier is offering complimentary identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Hoosier has also notified law enforcement.

Number of New Hampshire Residents Impacted

Hoosier has identified 20 New Hampshire residents who were potentially impacted by this incident.

Contact Information

Please direct all correspondence and questions to me.

Sincerely,

Mark E. Schreiber
(Enclosures)

HOOSIER
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-888-364-7633
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

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

April 14, 2023

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are sending you this notice because of a recent data security incident that occurred at Hoosier Racing Tire Corporation ("Hoosier") that may have involved your personal information.

WHAT HAPPENED?
Hoosier hired third-party vendors to build and operate its ecommerce website, including where payment card information was collected. We learned that unauthorized code was installed on this vendor-managed site between November 2020 and September 2022. This code may have captured personal information from you, including payment card details when you made a purchase on the website during this time period. Hoosier discovered the potential disclosure of your personal information on or about March 9, 2023.

Hoosier promptly instructed the operator of the website to remove the unauthorized code and to launch an investigation. A leading cybersecurity forensics firm was also engaged to assist in the investigation. We subsequently notified law enforcement.

WHAT INFORMATION WAS INVOLVED?
The personal information that the unauthorized individuals may have accessed includes:
.

WHAT WE ARE DOING
In response to the incident, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

HOW DO I ENROLL FOR THE FREE SERVICES?
We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-364-7633 or going to https://app.idx.us/account-creation/protect 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 July 14, 2023.

WHAT YOU CAN DO
In addition to enrolling in the identity monitoring services we have arranged on your behalf, we recommend that you review your personal account statements and credit reports to detect errors resulting from the security breach and immediately report any suspicious activity. We also encourage you to review the "Steps You Can Take To Further Protect Your Information" sheet enclosed with this letter, which contains important information on placing fraud alerts

and other important topics. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency and have information related to fraudulent transactions deleted.

MORE INFORMATION

We apologize for any inconvenience that this incident may cause you. You will find detailed instructions for enrollment on the enclosed "Steps You Can Take to Further Protect Your Information" 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 1-888-364-7633 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have. You may also contact us at Hoosier Racing Tire Corporation, Attn: Privacy Office, 65465 S.R. 931, Lakeville, IN 46536.

Sincerely,

Hoosier Racing Tire Corporation

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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.

Telephone. Contact IDX at 1-888-364-7633 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free (1-877-322-8228), or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies, including:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a Connecticut resident, you may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, calling 410-576-6491, or writing to Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, 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/.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226 (Toll-free within North Carolina) 919-716-6000.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and to the FTC.

If you are a Rhode Island resident, you can request additional information by contacting the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov/, (401) 576-6491. If you are, or suspect you are, a victim of identity theft, you may also obtain or file a police report by contacting your local police department to file a report. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.