

KING & SPALDING

King & Spalding LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
www.kslaw.com

Robert Hudock, Partner
Direct Dial: +1 202-626-5521
rhudock@kslaw.com

Adam Solander, Partner
Direct Dial: +1 202-626-5542
asolander@kslaw.com

February 28, 2024

Anthony Brown, Attorney General
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Via USPS Mail

Re: Notice of Security Incident Affecting Superior Performers, LLC

Dear Attorney General Brown,

We write on behalf of Superior Performers, LLC ("SP") regarding a security incident, for which we notified your office via webform available at <https://www.marylandattorneygeneral.gov/Pages/contactus.aspx> on February 26, 2024 and provided a courtesy copy via U.S. Mail on February 27, 2024.

Please be advised that SP sent notices, a copy of which is enclosed, to impacted residents via USPS First Class Mail on or about February 27, 2024.

Please do not hesitate to contact us if you have any questions regarding this letter.

Sincerely,

/s/ Robert Hudock
Robert Hudock

/s/ Adam Solander
Adam Solander

Encl.: Individual Notice Letter Template

Superior Performers, LLC
1214 Turrentine Street
Burlington, NC 27215

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Maildate>>

Re: NOTICE OF DATA BREACH

Dear <<Name 1>>:

Thank you for being a part of Superior Performers, LLC as a valued insurance agent. We are deeply grateful for our partnership and appreciate your continual hard work and contributions in serving the needs of your clients. In addition to valuing our relationships with agents like you, we also value your personal information and want to help ensure it is safe and protected. That's why, as a precautionary measure, we are notifying you about a recent data security incident.

Although we are unaware of any actual misuse of your information, we want to let you and other potentially affected agents know about the incident — and offer you tools and guidance to help protect your personal information from potential identity theft or other misuse.

What Happened?

On November 14, 2023, we detected some disruptions on our network. We promptly reviewed these disruptions and subsequently discovered potential activity of an unauthorized user. Our team immediately engaged third-party experts and launched a comprehensive investigation to determine the scope and impact of the incident and to analyze any potential impacted data. Through our investigation, we learned that an unauthorized party gained access to the Superior Performers' network and certain data. On January 12, 2024, we completed our initial analysis and determined that your personal information, including your Social Security number, was among the impacted data. While we are unaware of any actual misuse of this information, we think it is important that you know about this incident. Out of an abundance of caution, we are also providing you with services and tools to help you protect yourself. Those services are described below.

What Information Was Involved?

Based on our investigation to date, the data accessed includes some or all of the following data: your name, address, personal and business email address, telephone number, date of birth, and Social Security Number.

What Are We Doing?

Immediately upon learning of the security incident, we began reviewing all its aspects and took steps to protect the systems involved. We will continue to work with outside experts to assess the incident, including reviewing and enhancing our system security and administrative and technical safeguards.

As an additional measure of protection, we are providing you with complimentary credit monitoring services through Equifax.

What Can You Do?

As always, we recommend that you remain vigilant and review your account statements and free credit reports regularly and report any concerning transactions to your financial provider.

We encourage you to enroll in Equifax's Credit Watch Gold. You can also review the "Additional Resources" section of this letter for additional ways to help protect yourself. They include recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file.

For More Information

We regret any inconvenience or concern this incident may have caused. Please know that we remain as committed as ever to serving and supporting you. If you have questions about the incident, please contact the Superior Performers, LLC incident response line at 888-321-6125 available Monday through Friday, 9:00am – 9:00pm EST.

Sincerely,

Andy Albright

ADDITIONAL RESOURCES

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, including exercising your right to file a police report. You may also contact your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you 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 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at

<https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

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 90 days. 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>.

Credit Report Monitoring & Identity Theft Protection Services

In addition, Superior Performers, LLC has arranged with Equifax to provide you with credit monitoring and identify theft protection services for one year, at no cost to you. The Credit Watch Gold package provides you with the following benefits:

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

To take advantage of this offer, you must enroll by <<Enrollment Deadline>>, your code will not work after this date.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".

If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

State Information on Preventing and Responding to Identity Theft

You may want to review any materials your state provides regarding identity theft and credit monitoring that may provide additional information and resources to protect yourself against any risks. Below is a list of state resources that may be helpful to review for additional information.

District of Columbia residents: May obtain information on how to minimize identity theft risks provided by the Office of the Attorney General for the District of Columbia at <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>, or by calling (202) 727-3400 or writing to the Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001.

Florida residents: May obtain information on how to minimize identity theft risks provided by the Florida Attorney General at <https://www.myfloridalegal.com/identity-theft/identity-theft-victim-kit>.

Louisiana residents: May obtain information from the Louisiana Department of Revenue at <https://revenue.louisiana.gov/TaxFraud/IdentityTheft>. The Louisiana Department of Revenue also provides an "Identity Theft Checklist" at <https://revenue.louisiana.gov/FraudForms/IdentityTheftChecklist.pdf>.

Maryland residents: May 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, or writing to the Office of the Attorney General at 200 St. Paul Place, Baltimore, MD 21202, or calling 1-888-743-0023 (toll free) or 410-576-6491.

New Hampshire residents: May obtain information about steps for victims of identity theft from the Consumer Protection and Antitrust Bureau of New Hampshire's Department of Justice, Office of the Attorney general at <https://www.doj.nh.gov/consumer/identity-theft/index.htm>.

New Jersey residents: May obtain information about preventing identity theft from the Division of State Police in the Department of Law and Public Safety at <https://www.nj.gov/njsp/tech/identity.html>.

New Mexico residents: Consumers have rights pursuant to the Fair Credit Reporting Act (FCRA), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-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: May obtain information about preventing and responding to identity theft from the New York State Department of State Division of Consumer Protection at <https://dos.ny.gov/protecting-yourself-identity-theft>, which also links to a comprehensive guide <https://dos.ny.gov/system/files/documents/2018/06/idtheftbrochure.pdf>.

North Carolina residents: May obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

Texas residents: May obtain information on helping prevent identity theft provided by the Texas Attorney General at <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/help-prevent-identity-theft>.

Virginia residents: May obtain information by viewing the comprehensive guide for identity theft victims provided by the Virginia Attorney General at https://www.oag.state.va.us/consumer-protection/files/ID_Theft_Booklet_2016_web.pdf.

Washington residents: May obtain information by reviewing the "Identity Theft/Privacy" section of the Washington Attorney General's website at <https://www.atg.wa.gov/guardit.aspx>.

Wisconsin residents: May obtain information by reviewing Wisconsin's Department of Agriculture, Trade and Consumer Protection's ID Theft/Privacy Protection Fact Sheets at <https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx#:~:text=Credit%20Report%20Security%20Freeze,help%20protect%20from%20identity%20theft.>