



Lauren Godfrey
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
322 North Shore Drive
Building 1B, Suite 2100
Pittsburgh, PA 15212
lgodfrey@constangy.com
412.870.4129

April 3, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Department of Professional and Financial Regulation
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Original Footwear, Co. (“Original Footwear”), a footwear manufacturer located in Tennessee, in connection with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On February 3, 2024, Original Footwear became aware of unusual network activity and immediately took steps to secure its systems. Original Footwear also engaged cybersecurity experts to conduct an investigation to determine the scope of potential unauthorized activity and whether any sensitive or personal information may have been accessed or acquired. That investigation identified that certain Original Footwear data may have been acquired without authorization as a result of the incident. Following this discovery, Original Footwear undertook a preliminary review of the information that may have been involved in the incident. On February 19, 2024, Original Footwear identified that a limited amount of employee personal information was contained in the data. Since that time, Original Footwear has been working to gather contact information needed to provide notice to potentially affected individuals.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately 1 (one) Maryland resident. The information involved in the incident for the affected Maryland resident may have included name and Social Security number.

3. Notification to Affected Individual(s)

On April 3, 2024, notification letters will be sent to the affected Maryland resident by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the individuals the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center, should any individual have questions about the incident. A sample notification letter sent to the impacted individual(s) is included with this correspondence.

4. Steps Taken Relating to the Incident

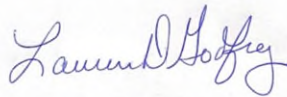
As soon as Original Footwear discovered this incident, it launched an investigation, took immediate steps to enhance the security of its network, and worked to determine whether any personal information was accessed or acquired without authorization. Original Footwear then worked diligently to determine what personal information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification. Original Footwear has additionally notified the FBI of the incident and is cooperating with the ongoing investigation.

Original Footwear is offering residents complimentary Experian IdentityWorks services for 12 months, including credit and identity monitoring services, identity restoration, and \$1,000,000 of identity theft insurance. Original Footwear has also established a call center through Experian for any of the individuals to reach out to, should the need arise.

5. Contact Information

Original Footwear remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lauren Godfrey at lgodfrey@constangy.com.

Sincerely,



Lauren Godfrey

Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter



Return Mail Processing
PO Box 999
Suwanee, GA 30024

3 1 887 *****AUTO**ALL FOR AADC 240

SAMPLE A. SAMPLE - Adult SSN

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



Subject: Notice of Data [Extra1]

April 3, 2024

Dear Sample A. Sample:

We are writing to inform you of a data security incident that may have affected your personal information. At Original Footwear Co. (“Original Footwear”), we take the privacy and security of personal information very seriously. That is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On February 3, 2024, Original Footwear became aware of unusual network activity and immediately took steps to secure our systems. We also engaged cybersecurity experts to conduct an investigation to determine the scope of potential unauthorized activity and whether any sensitive or personal information may have been accessed or acquired. That investigation identified that certain Original Footwear data may have been acquired without authorization as a result of the incident. Following this discovery, Original Footwear undertook a preliminary review of the information that may have been involved in the incident. On February 19, 2024, we identified that a limited amount of employee personal information was contained in the data. Since that time, we have been working to gather contact information needed to provide notice to potentially affected individuals.

What Information Was Involved. The potentially affected information may have included your name and Social Security number.

What We Are Doing. As soon as we discovered the incident we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever assistance is needed to hold the perpetrators accountable.

To help protect your identity, we are offering complimentary access to **Experian IdentityWorksSM** for **[Extra2]** months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra2] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra2]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** July 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-8030 by July 31, 2024. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra2] MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the Experian identity protection services, which are offered to you at no cost, using the instructions above. Please note the deadline to enroll in these complimentary services is July 31, 2024. Please do not discard this letter, as you will need the Membership Number provided above to access services.

For More Information. If you have further questions or concerns, or would like an alternative to enrolling online, please call 1-833-918-8030 toll-free Monday through Friday 8am to 8pm CST, closed Saturday and Sunday (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number]. Experian representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kevin Cole', with a stylized flourish at the end.

Kevin Cole

Original Footwear

5968 Commerce Blvd.

Morristown, TN 37814

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

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 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
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 respective 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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.