
CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

DAMON C. BARHORST, ESQ.
DBarhorst@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

July 11, 2024

Via E-Mail (IDTheft@oag.state.md.us)

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for United States Soccer Federation, Inc., located at 303 E. Wacker Drive, Suite 1200, Chicago, IL 60602, and write to inform you of a data security incident. By providing this notice, United States Soccer Federation does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around December 6, 2023, United States Soccer Federation ("US Soccer") became aware of potential unauthorized access into an email account belonging to an employee. Upon discovery, US Soccer took immediate action to address and investigate the event, which included engaging third-party specialists to assist with determining the nature and scope of the incident. A complete and thorough investigation confirmed that the employee's email account was subject to unauthorized access for a limited period of time between November 18, 2023 and December 4, 2023. US Soccer then began a review of the contents of the potentially affected email account to determine the type(s) of information contained within and to whom that information pertained. On April 1, 2024, following a thorough investigation, US Soccer determined that limited amount of information related to individuals was present in the email account. US Soccer then diligently worked to locate address information for potentially affected individuals and completed this process on May 22, 2024. Following completion of that address review, US Soccer concluded that limited amount of information related to one (1) Maryland resident was present in the email account.

On July 11, 2024, United States Soccer Federation provided written notice of this incident to the potentially impacted Maryland resident pursuant to Maryland law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to the individual is substantially similar to the letter attached hereto as Exhibit A.

Please contact me should you have any questions.

Very truly yours,



Damon Barhorst, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

United States Soccer Federation Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P
ZACHARY BAILOWITZ
511 FOREST ST
OAKLAND, CA 94618



July 11, 2024

Re: Notice of Data Breach

Dear Zachary Bailowitz:

United States Soccer Federation, Inc. is writing to inform you of an incident that may have involved some of your personal information. We take the privacy and security of data in our care very seriously and are providing information about the incident, our response, and steps you can take to help protect your information.

What Happened: On or around December 6, 2023, US Soccer became aware of potential unauthorized access into an email account belonging to an employee. Upon discovery, US Soccer took immediate action to address and investigate the event, which included engaging third-party cybersecurity specialists to assist with determining the nature and scope of the incident. An independent, complete and thorough investigation confirmed that the employee's email account was subject to unauthorized access for a limited period of time from November 18, 2023, to December 4, 2023. US Soccer, working with cybersecurity specialists, then began a review of the contents of the potentially affected email account to determine the type(s) of information contained within and to whom that information pertained. On April 1, 2024, following a thorough investigation and with the assistance of cybersecurity specialists, US Soccer determined that limited information related to individuals was present in the email account. US Soccer then diligently worked to locate address information for potentially affected individuals and completed this process on May 22, 2024.

What Information Was Involved: The potentially affected information may have included your first and last name, in combination with your Social Security number.

What Are We Doing? We have taken steps to address the incident and are committed to protecting the information entrusted to us. Upon learning of this incident, we immediately took steps to secure the email account and launched a thorough investigation. As an additional safeguard for your information, we arranged for you to enroll, at no cost to you, in an online credit monitoring service for 12 months. Due to state and federal privacy laws, we cannot enroll you directly. If you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself and additional information regarding how to enroll is enclosed. To enroll, we further recommend that you do so from a personal device.

What You Can Do. In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have also provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

000010102G0500

P

For More Information: Should you have any questions or concerns, you can call our dedicated assistance line at 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Sincerely,

United States Soccer Federation

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Instructions

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **F5A3E4DB05EC**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

United States Soccer Federation, Inc. may be contacted at 303 E. Wacker Drive, Suite 1200, Chicago, IL 60602.