



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

September 22, 2021

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP represents USA Swimming, the national governing body for the sport of competitive swimming. This letter is being sent because personal information for one New Hampshire resident may have been affected by a recent data security incident experienced by USA Swimming. The incident may have involved unauthorized access to such resident's name and passport number.

On June 30, 2021, USA Swimming learned of unusual activity associated with two USA Swimming employee email accounts. Upon learning of this activity, USA Swimming immediately took steps to secure its email environment and launched an investigation. In connection therewith, USA Swimming engaged a leading, independent forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. Through that investigation, USA Swimming learned that two employee email accounts were accessed without authorization. USA Swimming then engaged a vendor to conduct a review of the contents of the one email account potentially containing personal information. On August 13, 2021, USA Swimming learned that account contained certain personal information. USA Swimming then worked diligently to identify current address information required to notify potentially impacted of this incident. That process was completed on September 2, 2021.

Please note that this incident impacted only information transmitted via email and did not affect any other information systems. USA Swimming has no evidence of misuse of any potentially affected information.

USA Swimming notified the potentially affected New Hampshire resident of this incident via the attached sample letter on September 17, 2021.

Attorney General Gordon MacDonald
September 22, 2021
Page 2

Please contact me should you have any questions.

Very truly yours,



Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter



USA Swimming

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

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

September 17, 2021

Re: Notice of Data <<Variable 1>>

Dear <<FirstName>> <<LastName>>,

I am writing to inform you of a data security incident experienced by USA Swimming that may have impacted your personal information. USA Swimming takes the privacy and security of all information within its possession very seriously. This letter contains information about the incident and information about steps that you can take to help protect your personal information.

What Happened? On June 30, 2021, USA Swimming learned of unusual activity associated with two USA Swimming employee email accounts. Upon learning of this activity, USA Swimming immediately took steps to secure its email environment and launched an investigation. In connection therewith, USA Swimming engaged a leading, independent forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. Through that investigation, USA Swimming learned that two employee email accounts were accessed without authorization. USA Swimming then engaged a vendor to conduct a review of the contents of the one email account potentially containing personal information. On August 13, 2021, USA Swimming learned that account contained some of your personal information. USA Swimming then worked diligently to identify current address information required to notify you of this incident. That process was completed on September 2, 2021.

Please note that this incident impacted only information transmitted via email and did not affect any other information systems. In addition, USA Swimming has no evidence of misuse of any potentially affected information.

What Information Was Involved? The following information may have been impacted in connection with this incident: your <<Variable 2>>.

What We Are Doing. As soon as USA Swimming discovered this incident, USA Swimming took the steps referenced above. USA Swimming also applied enhanced security measures to its email system in order to help prevent a similar incident from occurring in the future. In addition, the Federal Bureau of Investigation is aware of this incident and USA Swimming will provide whatever assistance is necessary to hold the perpetrator(s) of this incident accountable.

What You Can Do. Although USA Swimming is not aware of any misuse of information as a result of this incident, USA Swimming encourages you to follow the recommendations on the following page to help protect your personal information.

For More Information. If you have questions, please contact IDX at 1-800-939-4170, Monday through Friday from 7 a.m. to 7 p.m. Mountain Time, excluding major US holidays. Call center representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Michelle Steinfeld
Secretary & General Counsel

USA Swimming, Inc.
1 Olympic Plaza
Colorado Springs, CO 80909-5780

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 can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. 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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.