NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

November 21, 2016

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, the United States Olympic Committee ("USOC"), to inform you of a potential security incident involving personal information provided to the USOC that may have affected approximately one New Hampshire resident. The USOC is notifying individuals and outlining some steps they may take to help protect themselves.

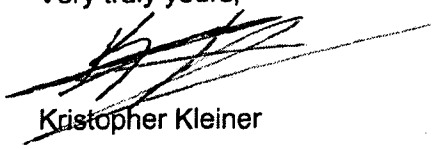
On November 18, 2016, the USOC learned that an unauthorized individual had gained access to an email sent to a government contractor who performed security clearances in advance of a USOC event. The email attachment contained certain personal information, including name, address, date of birth, telephone number, social security number and passport information for a limited number of individuals. Based on its investigation to date, the USOC has not identified any evidence that this incident involves any unauthorized access to or use of any USOC computer systems or networks.

The USOC takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Upon learning of the incident, the USOC promptly took steps to address the situation, including initiating an internal investigation of this incident and notifying federal law enforcement. Although it does not appear that this incident involves any USOC systems, the USOC will be retaining an independent computer forensics firm to confirm its internal findings and conduct a review of the its security practices, including the security procedures used when transmitting sensitive information to third parties.

Affected individuals are being notified via email and written letter and affected individuals will be offered complimentary identity protection and fraud resolution services. These notifications will begin mailing on or around November 20, 2016. Form copies of the notices being sent to the affected New Hampshire resident are included here for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,



Kristopher Kleiner

KCK
Enclosure

[USOC LETTERHEAD]

[DATE]

[NAME]

[ADDRESS]

Dear [NAME]:

Notice of Data Breach

We are writing to inform you of a security incident involving certain personal information you provided to the USOC. As detailed further below, it appears that this information was taken from a government contractor who helped to run security clearances for the 100-Days Out Event in April 2016. That contractor was not affiliated with the USOC and we are not aware of any evidence indicating that our systems were compromised. We are providing this notice as a precaution to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

On November 18, 2016, we learned that certain information you provided to the USOC prior to attending the 100-Days Out Event was acquired by an unauthorized person. It appears that unauthorized person was able to gain access to the email account of the government contractor who performed security clearances for certain attendees in advance of the Event. The unauthorized person then posted a number of the contractor's emails to a website, including an email that included your personal information provided as part of the clearance process. Based on our investigation we have not found any evidence that this incident involves any unauthorized access to or use of any USOC computer systems or networks.

What Information Was Involved

The information posted on the website includes your name, date of birth, address, telephone number, social security number and passport information. Please note that, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. Upon learning of this incident, we promptly took steps to address the situation, including initiating an internal investigation of this incident and notifying federal law enforcement. Although it does not appear that this incident involves any USOC systems, we will be retaining an independent investigator to confirm our internal findings and conduct a review of our security practices, including the security procedures used when transmitting sensitive information to third parties.

In addition, to help protect your identity, we will be offering complimentary identity protection services from a leading identity monitoring services company. These services will help detect possible misuse of your personal information and provide you with identity protection support focused on immediate identification and resolution of identity theft. We will have these

arrangements in place soon; you should expect to receive additional information about these services within the next few days.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office to file a police report for identity theft, and get a copy of it. You may need to give copies of the police report to creditors to help clear up your records.

As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you can take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

We understand the importance of keeping your sensitive personal information confidential and we sincerely regret any concern this situation causes you. We stand ready to support and assist you in addressing and resolving any questions or concerns you may have. If you need more information please feel free to contact us at: 719-866-2253 or DataQuestions@usoc.org. .

Sincerely,

Pam Sawyer
Managing Director – Human Resources
United States Olympic Committee

Information About Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241, Atlanta, GA 30374
800-685-1111
Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:
P.O. Box 2002, Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
P.O. Box 105281, Atlanta, GA 30348
877-322-8228
Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872