O'REILLY®

STATE OF NH
DEPT OF JUSTICE
2016 APR -4 AM 11:38

March 31, 2016

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster,

The O'Reilly Media Group is writing to notify you of an authorized access of personal information involving three (3) New Hampshire residents.

Nature of the Unauthorized Access
On February 11, 2016, the O'Reilly Media Group discovered that unauthorized access to a database backup file for the O'Reilly School of Technology had occurred. The incident was discovered as the O'Reilly Media Group was shutting down the O'Reilly School of Technology.

It appears that on November 13, 2015, a then student of the O'Reilly School of Technology copied a private database backup file. We cannot determine whether or not the then student reviewed the contents of the backup file or whether the file was copied to an external location. While the incident is still being investigated, at this time it does not appear to be a deliberate malicious attack.

The back-up file that was copied contained social security numbers, in combination with one or more of the following data elements, if they were previously provided to the O'Reilly School of Technology: name, email address, telephone number, birth date, and/or postal address.

Number of New Hampshire Residents Affected
This incident affected the personal information of three (3) individuals residing in New Hampshire. We will be notifying these individuals in writing about this incident on April 1, 2016. An exemplar copy of the notification letter is enclosed for your information.

To mitigate the risk to the affected New Hampshire residents O'Reilly Media Group is making available one (1) year of identity theft protection and recovery services, at no cost, through IdentityForce.

Steps Taken Related to the Incident
The discovery of the incident triggered our incident response process, which included a containment response, input from outside experts, and identification of forward-looking protocol and process changes.

The computer systems and networks for the O'Reilly School of Technology have now been completely shut down. A single copy of the database backup file has been retained in a highly secure environment for forensic purposes. We have monitored other areas of our network and we do not believe that there is ongoing risk. We remain vigilant in assessing and monitoring our security measures.

For any questions or additional information regarding this incident, please contact me.

Yours sincerely,

Kathy Lanterman
CFO

Enclosure: Sample copy of notification letter to New Hampshire residents

O'REILLY MEDIA, INC. oreilly.com @oreillymedia
SEBASTOPOL 1005 Gravenstein Highway North • Sebastopol, California 95472 • T (800) 998-9938 • T (707) 827-7000 • F (707) 829-0104
BOSTON 2 Avenue de Lafayette, 6th Floor • Boston, Massachusetts 02111 • T (800) 775-7731 • T (617) 354-5800 • F (617) 661-1116

To: [Full name]

From: O'Reilly Media, Inc.

Date: April 1, 2016

NOTICE OF DATA BREACH

What Happened?	On February 11, 2016, we discovered unauthorized access to a database backup file for the O'Reilly School of Technology ("OST"). It appears that a student of OST copied a private database backup file on November 13, 2015. We cannot determine whether or not the student reviewed the contents of the database backup file or whether the file was also copied to an external location. The contents of the database backup file included the personal information of some OST students. While the incident is still being investigated, at this time it does not appear to be a deliberate malicious attack.
What Information Was Involved?	The files that were copied contained your social security number, in combination with one or more of these data elements, if you provided them to us: name, email address, telephone number, birth date, and/or postal address.
What We Are Doing	The discovery of the incident triggered our incident response process, which includes a containment response, input from outside experts, and identification of forward-looking protocol and process changes. The incident was discovered as we were shutting down the OST business. The computer systems and networks for OST have now been completely shut down. We have monitored other areas of our network and do not believe there is ongoing risk. A single copy of the database backup file has been retained in a highly secure environment for forensic purposes. Independent of this incident, O'Reilly is improving its information security practices, policies, and controls. We will remain vigilant in assessing and monitoring our security measures and make additional changes as necessary.
What You Can Do	**Free Identity Protection And Credit Monitoring Services** To mitigate your personal risk, we are making available to you one year of identity theft protection and recovery services at no cost through IdentityForce.

We strongly encourage you to enroll in, and take advantage of, this free service.

To sign up online please visit: https://secure.identityforce.com/benefit/oreilly

Step 1: Enter your ***First and Last Name***
Step 2: Enter your ***Email Address***
Step 3: Enter your ***Verification Code:*** [insert verification code]
Step 4: Click Continue button
Step 5: Enter the required information on the Personal Information page

To enroll by phone, please contact IdentityForce Membership Services at 1-877-MYIDFORCE (1-877-694-3367), Monday through Friday 8:30 AM to 5:30 PM ET. You will need to have your Verification Code handy when you call.

While we encourage you to enroll in this free service soon, you may enroll anytime within 12 months after you receive this letter.

Additional Steps To Protect Yourself

Monitor Your Credit Reports: We recommend that you review your account statements and monitor credit reports. Under federal law, you are entitled to obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. You can request your report online at www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or mail 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 can also contact each credit reporting agencies at the addresses below:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
Fraud Hotline: 1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
Fraud Hotline: 1-888-397-3742
www.experian.com

Transunion
P.O. Box 2000
Chester, PA 19022
Fraud Hotline: 1-800-888-4213
www.transunion.com

If you suspect your information has been fraudulently used, notify IdentityForce Membership Services at 1-877-MYIDFORCE (877-694-3367), Monday through Friday 8:30 AM to 5:30 PM ET.

You should also report the incident to proper law enforcement authorities, your state's attorney general, and/or the Federal Trade Commission ("FTC").

You may contact the FTC to obtain additional information, at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (or 1-877-438-4338)
www.ftc.gov/idtheft

Fraud Alert: You may also place a fraud alert on your credit report by contacting any one of the three national credit reporting agencies listed above. A fraud alert lasts 90 days. It makes it more difficult for someone to get credit in your name because it requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name. If you become a victim of identity theft, you may extend the fraud alert on your credit report subject to documentation that the credit reporting agency may request from you. Once you have requested an alert with one agency, the other two agencies will be automatically notified.

Credit Freeze: You may also place credit freeze (also called a security freeze) on your credit file, so that no new credit can be issued in your name without the use of a personal identification number (PIN) or password, or both, issued to you when you initiate a credit freeze. Please note that if you do initiate a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Accordingly, using a credit freeze may delay your ability to obtain credit, such as applying for a credit card or a loan.

Credit freeze laws vary from state to state, and are subject to different costs (including the costs to initiate the freeze, temporarily lifting of the freeze, and permanently removing the freeze). Certain state laws may also provide residents of that state with free credit freeze services if a person can verify that he or she is a victim of identity theft (and provide documentary proof, such as a police report), or if a person is requesting the credit freeze for the first time. We therefore recommend that you contact the major credit reporting agencies listed above for more information.

For a chart of the fees that may be charged, and other information regarding the specific requirements of each state, please see, for example:

https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements
http://www.experian.com/consumer/security_freeze.html
http://www.transunion.com/securityfreeze?tab=freezefees

For More *Information*	**How to Place a Fraud Alert and/or Request a Credit Freeze?** To place a fraud alert or request a credit freeze, you must contact one of the three major credit reporting agencies: **Equifax:** 800-525-6285, www.equifax.com **Experian:** 888-397-3742, www.experian.com **TransUnion**: 800-680-7289 www.transunion.com The credit reporting agency may request that you provide specific detailed information about you, in order to identify you. Thus, be prepared to provide detailed information about you, such as: • Full name, address, social security number and date of birth • Addresses where you have lived in the past five years • Proof of current address such as a current utility bill or phone bill • Photocopy of a government issued identification card • Copy of police report, investigative report, or complaint to law enforcement regarding the incident. **How to Temporarily or Permanently Remove a Credit Freeze** To temporarily lift the credit freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include proper identification (name, address, and SSN) and the PIN number or password provided to you when you placed the credit freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report to be available. The consumer reporting agencies have three business days after receiving your request to lift the credit freeze for those identified entities or the specified period of time. To remove the credit freeze permanently, you must send a written request to each of the credit reporting agencies by mail and include proper identification (name, address, and SSN) and the PIN number or password provided to you when you placed the credit freeze. The credit bureaus have three business days after receiving your request to remove the credit freeze. **Information about Identity Theft** For additional information about fraud alerts, credit freezes, and steps you can take to protect against identity theft, visit the website of the U.S. Federal Trade Commission at: www.identitytheft.gov You can also write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580, call Toll-Free: 1-877-IDTHEFT (or 1-877-438-4338); or Visit: http://www.consumer.ftc.gov/features/feature-0014-identity-theft **Additional Precautions** Whether or not you take advantage of the free services being offered above and/or obtain assistance directly from the credit reporting agencies as described above, we encourage you take these additional precautions to protect against identity theft:

1. Remain vigilant and regularly review all of your account statements (including but not limited to your bank, credit card, and social security accounts, and monitor free credit reports for any unusual activity).

2. Be alert to "phishing" by someone who attempts to contact you and requests sensitive information over email or one the phone, such as password, social security numbers (or part of it), or bank account numbers.

3. Immediately report any suspected incidents of identity theft to local law enforcement agencies

Be Watchful of Scammers

When an incident occurs, such as the one that is the subject of this letter, scammers may try to find ways to contact the individuals affected by the incident to scare them, ask questions, or pretend to offer services. Their actual purpose is to deceive victims into disclosing confidential personal information.

Please be vigilant. If at any time, someone whom you do not recognize contacts you and requests any information regarding this incident, or pretends to be: (1) from O'Reilly Media, Inc., (2) an agent or representative of O'Reilly Media, Inc., or (3) offering services as a result of this incident (e.g. asks you what you received, or to provide other personal information, etc.), please:

- Do not respond to any questions, and do not provide any information;
- Tell that person that all his/her inquiries should be directed to customercare@oreilly.com or (707) 827-7300 and
- Contact us as soon as possible to inform us of this inquiry using the contact information provided below.

We will never contact you by email or by phone to ask you to provide sensitive information such as a social security or a driver's license number.

We are so sorry that this incident occurred. We hope that the information contained in this letter, and the identity theft and credit monitoring service that we are making available, will be useful to you. If you have any questions or concerns, please contact us at customercare@oreilly.com or (707) 827-7300 and we will address your questions as quickly as possible.