



Aubrey L. Weaver
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Aubrey.Weaver@lewisbrisbois.com
Direct: 215.253.7506

May 6, 2022

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Incident

Dear Attorney General Formella:

We represent the University of Southern California (“USC”), a private research university located in Los Angeles, California. This letter is being sent because personal information belonging to a New Hampshire resident may have been involved in a potential data security incident. The potentially affected information included the New Hampshire resident’s social security number.

On October 1, 2021, USC learned that a professor misplaced an external hard drive on or about September 28, 2021. In response, USC initiated an investigation and a review of available backups of the hard drive data to identify whether it contained personal information. The investigation determined that the hard drive contained academic information, including grade sheets and other similar documents, for certain current and former USC students, after which USC undertook efforts to identify all potentially affected individuals. USC’s review of the potentially affected data concluded in March 2022, at which time it identified one (1) New Hampshire resident whose information may have been involved.

USC has no evidence that any information involved in this incident has been misappropriated. Out of an abundance of caution, USC notified the potentially affected New Hampshire resident of this incident via the attached sample letter on April 26, 2022. In so doing, USC offered the notified New Hampshire resident complimentary identity protection services through IDX, a data incident and recovery services expert. These services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

May 6, 2022
Page 2

USC takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-7506 or Aubrey.Weaver@lewisbrisbois.com.

Sincerely,

A handwritten signature in black ink, appearing to be 'Aubrey L. Weaver', with a stylized, cursive script.

Aubrey L. Weaver of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

University of Southern California
Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



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

To Enroll, Please Call:
1-833-820-0961
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

April 26, 2022

Re: Notice of Data <<Variable 1>>

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

We are writing to provide you with information about a recent data security incident that may have involved your personal information. At the University of Southern California (“USC”), we strive to maintain the privacy and security of all information within our possession. As explained below, we have no evidence that your information has been misappropriated. Out of an abundance of caution, however, we are writing to notify you of this incident, offering complimentary identity monitoring and identity theft restoration services, and informing you about steps you can take to help safeguard your personal information.

What Happened. On October 1, 2021, USC learned that a professor lost an external hard drive on or about September 28, 2021. In response, USC initiated an investigation and a review of available backups of the hard drive data to identify whether it contained personal information. The investigation determined that the hard drive contained student academic information, including grade sheets and other similar documents. At that time, we launched a comprehensive review of the data stored on the device and took steps to gather contact information needed to provide notification to potentially affected individuals. This process concluded in March 2022 and determined that some of your personal information may have been stored on the hard drive.

As referenced above, USC is not aware of any misuse of information stored on the lost hard drive. Nonetheless, out of an abundance of caution, we are notifying you of this incident and offering resources to help you protect your personal information.

What Information Was Involved. The potentially affected information may have included your <<variable text>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. USC has also reviewed its data security policies with the professor in an effort to prevent a similar incident occurring in the future.

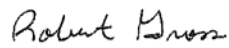
Additionally, USC is providing you with information about steps that you can take to help protect your personal information and, as an added precaution, is offering you complimentary identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<membership offering length>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The deadline to enroll is July 26, 2022.

What You Can Do. We recommend that you activate your complimentary IDX services using the enrollment code provided above. A description of the services being provided are included with this letter. We also recommend that you review the guidance included with this letter about steps you can take to protect your personal information.

For More Information. If you have questions or need assistance, please contact IDX at 1-833-820-0961, Monday through Friday from 6:00 am to 6:00 pm Pacific Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

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

Sincerely,

A handwritten signature in cursive script that reads "Robert Gross".

Robert (Bob) Gross
Director, Data Privacy

University of Southern California
Office of Culture, Ethics and Compliance,
University Gardens Building, Suite 105,
Los Angeles, CA 90089-8007

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/articles/pdf-0096-fair-credit-reporting-act.pdf>.