



Office of the UCLA Chief Privacy Officer

July 31, 2017

BY U.S. MAIL

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

RECEIVED
AUG 04 2017
CONSUMER PROTECTION

To: New Hampshire Attorney General Joseph Foster

UCLA is reporting a cyberattack against a server in its Summer Sessions and International Education Office that contained personal information provided by students, such as their names, addresses, dates of birth, Social Security numbers, health insurance subscriber IDs, and some medical information self-reported by students (e.g., allergies, medical conditions, medications). Extensive forensic analysis of the attack does not show that the attacker actually accessed or acquired any personal information on the server. However, we cannot conclusively rule out that possibility.

I am writing to make you aware that 27 residents of New Hampshire were among the affected population.

On July 31, 2017, UCLA began providing notification to potentially affected individuals by U.S. Mail and offering eligible individuals 12 months of identity protection services at no cost. The notice should be received within the next few weeks. A copy of the notice is enclosed.

Further information can be found at <https://www.it.ucla.edu/security/ss-ieo>. Should you have questions, I can be reached at kent@ucla.edu or (310) 206-3874.

Sincerely,

Kent Wada
UCLA Chief Privacy Officer

/encl



[RETURN MAIL ADDRESS]

[First_Name] [Last_Name]
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

«Date»

Dear «Parent or Guardian of» «First_Name» «Last_Name»,

At UCLA Summer Sessions & International Education, the confidentiality and security of student records and personal information is important to us. Unfortunately, our program was the victim of a cyberattack that may have put some of your «child's» personal information at risk. On May 18, 2017, we determined that an attacker gained unauthorized access to a Summer Sessions & International Education Office server that contained personal information provided by students, such as their names, addresses, dates of birth, social security numbers, health insurance subscriber IDs, and some medical information self-reported by students (e.g., allergies, medical conditions, medications, etc.). Extensive forensic analysis of the attack does not show that the attacker actually accessed or acquired any personal information on the server. However, we cannot conclusively rule out that possibility.

Although we have no evidence that your «child's» information was accessed or acquired by an unauthorized person, we have determined that the database contained your «child's» «social security number» «health insurance and/or medical information» «social security number and health insurance and/or medical information». In order for you to protect «yourself» «your child», we have arranged to have AllClear ID provide eligible individuals with identity protection services **at no cost**. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.


- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» and a dedicated investigator will help recover financial losses, restore your credit and medical records, and make sure your identity is returned to its proper condition.
- AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up at <https://enroll.allclearid.com> or by calling «DID_Phone» using the following redemption code: {RedemptionCode}. Please keep this code available should you need to call AllClear ID in the future.

Please note: You may be required to take additional steps in order to activate your phone alerts and monitoring options.

There are other things you can do to help protect «yourself» «your child». Please see the “Information about Identity Theft Prevention” attachment for information about how you can place a fraud alert and/or credit freeze on «your» «your child’s» credit file and how you can obtain a free copy of «your» «your child’s» credit report.

I am sorry that this incident occurred. All of us at UCLA take seriously our responsibility to protect personal information entrusted to us. We have made modifications to the server to help protect against another cyberattack, and we continue to work diligently to strengthen the security of our systems. If you have questions about any of the services being provided, please visit <https://www.it.ucla.edu/security/ss-ieo> or call the incident response line at 1-855-801-1252 (from within the U.S.) or +1 512-201-2203 (international), Monday through Saturday, 6 a.m. to 6 p.m. Pacific Time (excluding U.S. national holidays).

Sincerely,

A handwritten signature in black ink that reads "Jaime Balboa". The signature is written in a cursive style with a large, stylized 'J' and 'B'.

Jaime Balboa, Ph.D.
Assistant Vice Provost
Summer Sessions, Communications, and External Partnerships

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 below.

Equifax: P.O. Box 740241, Atlanta, GA 30374-0241, 1-800-685-1111, 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 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and social security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and 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 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 Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the 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

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. **If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.**

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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): 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:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

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

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; social security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

2017 AUG -4 AM 11:28
STATE OF NH
DEPT OF JUSTICE