McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

September 5, 2014

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: California State University, East Bay – Incident Notification

Dear Attorney General Delaney:

We represent California State University, East Bay ("CSUEB") and are writing to notify you of a data privacy incident that affects the security of personal information of two (2) New Hampshire residents. CSUEB's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission. By providing this notice, CSUEB does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On August 11, 2014, the CSUEB discovered that unauthorized access to personal information occurred on August 23, 2013. Upon discovery of the incident, CSUEB immediately commenced an internal investigation. Based on CSUEB's findings to date, CSUEB has learned that an unknown third-party broke into a CSUEB web server using an overseas IP address and a software tool designed to secretly access information on the server. The particular campus server affected was used to store various employment transaction records and some extended learning course information. The malicious files have been removed from the server and vulnerabilities have been mitigated.

Since completing the forensic investigation, CSUEB has devoted considerable time and effort to determine what exact information may have been on the affected server. CSUEB can confirm that the malicious software tool allowed the unauthorized individual to copy a data file containing the residents' full names, addresses, and Social Security numbers. No financial, banking, academic, or medical information was included in the data file.

To date, CSUEB is not aware of any reports of identity fraud resulting from this incident nor does CSUEB have any evidence to suggest that personal information has actually been misused. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps CSUEB is taking to safeguard the residents against identity fraud.

CSUEB provided the New Hampshire residents with written notice of this incident on September 5, 2014, in substantially the same form as the letter attached hereto. CSUEB has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. CSUEB is also offering the residents a complimentary one-year membership with a credit monitoring service and is also providing dedicated call center support, to answer questions. CSUEB has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Maintaining the privacy of personal information is of the utmost importance to CSUEB and it has taken immediate steps to reevaluate its information security practices to help prevent similar incidents in the future.

Should you have any questions regarding this notification or the incident, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

JJG/dap
Encl.

CALIFORNIA STATE
UNIVERSITY
EAST BAY
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>><<ZIP>>

<<DATE>>

Dear <<First Name>><<Last Name>>:

The security and privacy of the personal information you provide to California State University, East Bay, is of utmost importance to us. Regrettably, we are writing to inform you of an incident involving the disclosure of some of that information.

On August 11, 2014, the University discovered that unauthorized access to your personal information occurred on August 23, 2013. Upon discovery of the incident, we immediately commenced an internal investigation. Based on our findings to date, the University has learned that an unknown third-party broke into a University web server using an overseas IP address and a software tool designed to secretly access information on the server. The particular campus server affected was used to store various employment transaction records and some extended learning course information. The malicious files have been removed from the server and vulnerabilities have been mitigated.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been on the affected device. We can confirm that the malicious software tool allowed the unauthorized individual to copy a data file containing your full name, address, and Social Security number. No financial, banking, academic, or medical information was included in the data file.

We deeply regret that this incident has occurred. To date, we are not aware of any reports of identity fraud resulting from this incident nor do we have any evidence to suggest that your personal information has actually been misused. The University, however, wanted to make you aware that your personal information may be in the possession of an unauthorized individual and explain the steps we are taking to safeguard you against identity fraud and suggest steps that you should take as well.

Enclosed you will find instructions on enrolling in a complimentary 12-month credit monitoring service along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/ or Security Freeze, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

California State University, East Bay has taken immediate steps to reevaluate our information security practices to help prevent similar incidents in the future. **If you have any further questions regarding this incident, please call our toll-free number we have set up to respond to questions at (888) 738-3759.** The call center is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Sincerely,

Brad Wells

Brad Wells
Vice President, Administration and Finance
and Chief Financial Officer

INSTRUCTIONS

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to California State University, East Bay. In response to this incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at our expense. This protection is provided by Experian, one of the three major nationwide credit

Activate Experian's® ProtectMyID® Now in Three Easy Steps:

1. ENSURE that you enroll by **December 5, 2014**.
2. VISIT the ProtectMyID Web Site to enroll: **www.protectmyid.com/redeem**
3. PROVIDE your 9-character Activation Code: <XXXXXXXXX>

If you have questions or need an alternative to enrolling online, please call (877) 371-7902 and provide Engagement #

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (877) 371-7902.

2. Placing a 90-Day Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts in your name, increase the credit limit on an existing account, or provide a new card on an existing account. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

TransUnion	**Experian**	**Equifax**
Consumer Fraud Division	Consumer Fraud Division	Consumer Fraud Division
PO Box 6790	PO Box 9554	PO Box 740256
Fullerton, CA 92834-6790	Allen, TX 75013	Atlanta, GA 30374-0256
www.transunion.com	www.experian.com	www.equifax.com
1-800-680-7289	1-888-397-3742	1-800-525-6285

3. **Consider Placing a Security Freeze on Your Credit File.**

In addition, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit report online at **www.annualcreditreport.com**.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. **Additional Resources.**

Social Security Office: www.ssa.gov/pubs/10064.html