Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

One Oxford Centre
301 Grant Street, 20th Floor
Pittsburgh, PA 15219-1410
T 412 562 8800
F 412 562 1041
www buchananingersoll com

Matthew H. Meade
412 562 5271
matthew meade@bipc com

December 15, 2010

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

SECURITY BREACH NOTIFICATION

Dear Mr. Delaney:

I am writing to you on behalf of my client Education Management Corporation ("EDMC"), one of the largest providers of private post-secondary education in North America. EDMC is providing notice pursuant to N.H. Rev. Stat. Ann. §§ 359-C:20 of a data security incident. EDMC found the Social Security number, name and address of four New Hampshire residents, together with information of other students and employees, on a password protected, company-issued laptop stolen from the California home of one of the deans of EDMC's Art Institute system of schools.

On September 20, 2010, when EDMC learned that the laptop had been stolen it understood that the laptop had been encrypted pursuant to EDMC policy which meant that any data on the laptop was secure and could not be accessed without the encryption key. On October 20, 2010, as part of EDMC's routine follow up of the theft, it learned that the data was not encrypted due to a technical issue with the encryption process. As soon as EDMC learned that the data on the laptop was not properly encrypted, EDMC immediately began the process of determining whether Social Security numbers were on the laptop. Then, once EDMC found Social Security numbers and names, it began to search for addresses so that notices could be sent. Much of the information on the laptop was dated, such that identifying current addresses of all individuals whose data was on the laptop was a time-consuming process.

As a result of EDMC's investigation, it has taken steps to address the incident and prevent any unauthorized use of personal information by reminding all of its schools of EDMC's policy for timely reporting the theft of a laptop, reminding all administrators about EDMC's policies regarding the storage of personal information on laptops, and taking steps to address any issues associated with encrypting laptops.

EDMC has no evidence that any information stored on the laptop has been misused. Out of an abundance of caution, and because protecting personal information is important to EDMC,

EDMC has arranged for all individuals whose personal information was stored on the laptop to enroll, at no cost, in an online 3-bureau credit monitoring service for one (1) year provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. EDMC notified the individuals impacted by this incident via US Mail on December 4, 2010. A copy of the notice sent to the four New Hampshire residents is attached hereto.

Please do not hesitate to contact me at [redacted] if you have questions or concerns.

Very truly yours,

Matthew H. Meade

MHM/
Enclosure

Return mail will be processed by: IBC
P.O. Box 802
Fort Mill, SC 29716-0802
PO #5018
10 11 00002210 789099

The Art Institute of California™-Inland Empire

674 East Brier Drive
San Bernardino, CA 92408-2800

[redacted]

December 3, 2010

Re: DATA SECURITY INCIDENT

Dear [redacted]

On September 20, 2010, Education Management Corporation ("EDMC") learned that a company-issued, password protected laptop was stolen from the home of one of our deans at The Art Institute of California - Inland Empire. When we first learned of the incident we believed that the laptop had been encrypted pursuant to EDMC policy. On October 20, 2010, we discovered that the encryption had not been effective on the laptop. On October 22, 2010, EDMC learned that that the laptop contained the names, addresses and Social Security numbers of current and former students and employees within our Art Institute system of schools. You are receiving this letter because your name and Social Security number were found during our analysis of the back-up of the data stored on the laptop. Although we have no evidence that your personal information has been accessed, misused or disclosed, we are notifying you so that you can take additional steps to protect your personal information, if you feel it is necessary. We also want to assure you that none of your savings, checking or credit card account numbers were found on the laptop.

This is a serious matter, and we have taken aggressive steps to address it and prevent any unauthorized use of your personal information. As soon as we learned of the incident and the fact that the data stored on the laptop was not properly encrypted, we began a thorough investigation of all data on the laptop. In order to help prevent a recurrence of an incident like this, we have reminded all of our schools of EDMC's policy for timely reporting the theft of a laptop, reminded all administrators about our policies regarding the storage of personal information on laptops, and taken steps to address our laptop encryption process.

Out of an abundance of caution, and because protecting your personal information is important to us, we have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service for one (1) year provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. To enroll in this service, go to the TransUnion Interactive Web site at **www.transunionmonitoring.com** and in the space referenced as "Activation Code", enter [redacted] and follow the simple steps to receive your services online within minutes. **If you choose to enroll in this service, you must activate your credit monitoring membership by February 28, 2011.**

If you have any questions regarding this incident, are concerned that you may have an identity theft issue, or do not have access to the Internet and wish to enroll in a similar offline, paper based, 3-bureau credit monitoring service, please call 1-800-242-5181 Monday through Friday, 9:00 a.m. to 7:00 p.m. Eastern time. When prompted, please enter or say the following six digit telephone pass code 456987. (Closed on all U.S. observed holidays) You can sign up for the online or offline credit monitoring service anytime between now and February 28, 2011. Due to privacy laws, we cannot register you directly.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily 3-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraudulent activity, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes up to $25,000 in identity theft protection with $0 deductible. (Certain limitations and exclusions may apply).

Whether or not you choose to use TransUnion Interactive's credit monitoring services, we recommend

that you regularly review your credit reports for any unauthorized activity. If you see anything you do not understand (for example, accounts you did not open, inquiries from creditors that you did not initiate, or personal information, such as home address and Social Security number) we recommend that you call your local law enforcement office, file a police report of identity theft, and obtain a copy of the police report, as you may need to give copies of the police report to creditors to clear up your records. Even if you do not find any signs of fraud on your reports, you should remain vigilant for incidents of fraud and identity theft and check your credit reports regularly.

You may also obtain a copy of your credit report, free of charge annually, directly from each of the three nationwide credit reporting companies. To order your free report, visit www.annualcreditreport.com, or call toll free at 1-877-322-8228, or write to the following addresses:

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

You also have the right to ask that the nationwide credit reporting companies place a Fraud Alert on your credit file to let potential credit grantors know to verify your identification before extending credit in your name in case someone is using your information without your consent. This is a free service and must be renewed every 90 days. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You can call one of the three major nationwide credit reporting companies to place your initial 90 day Fraud Alert: TransUnion 1-800-680-7289; Equifax 1-800-525-6285 or Experian 1-888-397-3742. As soon as the credit reporting company confirms your Fraud Alert they will also forward your alert request to the other two credit reporting companies so you don't need to contact them separately.

To learn more about how to protect against identity theft, please visit the Federal Trade Commission's Web site http://www.ftc.gov/idtheft or call the Federal Trade Commission at 1-877-IDTHEFT (1-877-438-4338) or write at:
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

On behalf of EDMC, I extend my sincerest apologies for any inconvenience this incident may cause. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact TransUnion at 1-800-242-5181 Monday through Friday, 9:00 a.m. to 7:00 p.m. Eastern time. When prompted, please enter or say the following six digit telephone pass code 456987. (Closed on all U.S. observed holidays)

Sincerely,

Emam El-Hout
President
The Art Institute of California - Inland Empire
(909) 915-2100