VEDDER PRICE®

222 NORTH LASALLE STREET
CHICAGO, ILLINOIS 60601
T: +1 (312) 609 7500
F: +1 (312) 609 5005

CHICAGO • NEW YORK • WASHINGTON, DC
LONDON • SAN FRANCISCO • LOS ANGELES

BRUCE A. RADKE
SHAREHOLDER
+1 (312) 609-7689
bradke@vedderprice.com

February 5, 2016

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Joseph Foster
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Breach Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General Foster:

We represent the University of Central Florida ("UCF") in connection with a recent intrusion into the university's computer network that resulted in unauthorized access to certain personal information of past and present UCF students as well as current and former university employees. The investigation of this incident is ongoing, and this notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. By providing this notice, UCF does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction in connection with this incident.

Background of the Incident

UCF was founded in 1963 and is located in Orlando, Florida. UCF and its 13 colleges provide opportunities to 63,000 students, offering 210 degree programs from UCF's main campus, hospitality campus, health sciences campus and its 10 regional locations. Further information about UCF is available at http://www.ucf.edu/about-ucf.

On January 15, 2016, UCF discovered the unauthorized access to a database containing personal information related to forty-three (43) New Hampshire residents who are current and former university employees in a category known as Other Personnel Services ("OPS"). Examples of positions in this category include, but are not limited to, undergraduate student employees (including those in work-study positions), graduate assistants, housing resident assistants, adjunct faculty instructors, student government leaders and faculty members who have

been paid for dual compensation/overload (for example, teaching additional classes). Employees who previously held but do not currently hold OPS positions may be included in this group of affected OPS employees. The personal information involved with respect to the OPS employees includes their first and last names, Social Security numbers and UCF-issued employee identification numbers.

Although UCF's investigation is ongoing, it does not appear that the affected database contained credit or debit card information, or other financial or medical information. Additionally, it does not appear that any other databases on the university's computer network that store personal information of New Hampshire residents were compromised as a result of this incident.

Upon learning of the incident, UCF promptly launched an internal investigation and reported the incident to law enforcement. UCF also engaged the Verizon RISK Team, a division of Verizon and a leading incident response and digital forensics firm, to assist in UCF's internal investigation.

Notice to New Hampshire Residents

On February 5, 2016, UCF will be notifying the affected New Hampshire residents of the incident. Attached is a sample of the notification letter that is being sent to the affected New Hampshire residents via first-class United States mail.

UCF has also arranged to offer one (1) year of complimentary credit monitoring and identity theft protection services through Experian to the affected New Hampshire residents.

In addition, UCF has established a call center (877-752-5527) that affected New Hampshire residents can contact between 9:00 a.m. and 9:00 p.m. Eastern time Monday through Friday to ask questions and to receive further information regarding the incident. UCF has also established a website (UCF.edu/datasecurity) that affected New Hampshire residents can access to receive helpful information, including, but not limited to, how they can protect themselves against identity theft and fraud.

Other Steps Undertaken and to Be Undertaken by UCF

UCF has already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include enhancing user account and password security, expanding the campus-wide information security awareness and training program, and strengthening data security processes and protocols on the UCF network.

Contact Information

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Very truly yours,

Bruce A. Radke

BAR/bah
Enclosures
cc: W. Scott Cole, Vice President and General Counsel, University of Central Florida
Shainoor Ladha-Karmali, Associate General Counsel, University of Central Florida

University of Central Florida

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>,

The University of Central Florida wants to make you aware of an intrusion into the university's computer network that resulted in the unauthorized access to your personal information. While we have no evidence to suggest that any of your information has been used inappropriately, we want to provide you with guidance on how you can protect yourself.

On January 15, 2016, UCF discovered the unauthorized access to a database containing the following personal information related to you: your first and last name, Social Security number and UCF-issued employee identification number. The database did not include your credit card information or other financial information.

Upon learning of the incident, UCF immediately launched an internal investigation and reported the incident to law enforcement. We have also engaged a leading incident response and digital forensics firm to assist in our internal investigation. In addition, we have already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include enhancing user account and password security, expanding the campus-wide information security awareness and training program, and strengthening data security processes and protocols on our network.

We encourage you to take advantage of the complimentary one-year credit monitoring and identity protection services we are offering you through Experian's® ProtectMyID® Alert. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided with this letter.

We take the security of your personal information very seriously, and we want to ensure you can get the answers to any questions you have. You can call 877-752-5527 between 9 a.m. and 9 p.m. EST Monday through Friday, and operators will be able to assist you in English or Spanish. We also have established a website to answer questions: UCF.edu/datasecurity.

We value the trust you place in UCF to protect the privacy and security of your personal information, and we regret any inconvenience or concern that this incident might cause you.

Sincerely,

Joel L. Hartman

Dr. Joel L. Hartman
Vice President, Information Technologies & Resources and CIO
University of Central Florida

Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: May 8, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: <<ACTIVATION_COD>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #PC98989.

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 and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity 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; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data 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.

Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8057 to register with the activation code above.

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 877-288-8057.

*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and is 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.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by 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 can print a copy of the request form at: https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at: http://www.annualcreditreport.com.

Credit and Security Freezes: 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 Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 6790
		Fullerton, CA 92834

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

Iowa Residents: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
and on-line at: http://www.iowaattorneygeneral.gov/.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft at:

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
and online at: www.oag.state.md.us

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
and online at: www.ncdoj.com