



# UNIVERSITY *of* NEW HAMPSHIRE

August 17, 2007

Office of the Attorney General  
Consumer Protection and Antitrust Bureau  
33 Capitol Street  
Concord, New Hampshire 03301  
Attn: Lauren Noether

Dear Ms. Noether:

This is notification from the University of New Hampshire about an electronic data security breach. This letter is intended to comply with New Hampshire statute (RSA 359-C20), which requires such notice to the Attorney General's Office.

A Microsoft Excel spreadsheet containing names and social security numbers of 29 New Hampshire residents who are graduate students at the University was posted within the university web site on or about April 17, 2007.

The University is preparing notices to all graduate students identified in the file. A copy of the notice is attached. Our intent is to mail these notices on Friday, August 17, 2007.

Please let me know if you have any questions about this matter.

Sincerely,

Thomas L. Franke  
Chief Information Officer/Asst. Vice President

Attachment

cc: Ron Rodgers, General Counsel



# UNIVERSITY of NEW HAMPSHIRE

16 August 2007

<<Fname>><<MI>><<Lname>>  
<<PMStreet Line 1>>  
<<PMStreet Line 2>>  
<<PMStreet Line 3>>  
<<PMCity>>, <<PMState>> <<PMZIP>>

Dear <<Fname>>,

The purpose of this letter is to notify you that information identifying you individually was inappropriately made available on the university's web site recently. The University of New Hampshire deeply regrets this error in handling your personal information.

In this letter I will try to explain what happened and what steps we have taken and what steps we will take in an effort to minimize the potential for harm as a result of this error. Additionally, although we have no way to know whether your data were accessed for purposes of misuse, I will offer some suggestions about steps you might want to take to further protect your identity. Finally, I will provide contact information for follow up communication on this issue.

### ***Background: What happened?***

A Microsoft Excel spreadsheet containing the credit hour and tuition information associated with "inter-college" graduate programs was posted to a university web site on or about April 17<sup>th</sup>, 2007, by a staff member who intended to make budget information available to other university staff who work with these budgets. In addition to the credit hour and tuition information that were visible at the top of the spreadsheet, the bottom of the report also included the names and social security numbers of students who were participating in these "inter-college" graduate programs.

Office of the Vice President for Student and Academic Services

Thompson Hall 105 Main Street Durham, New Hampshire 03824-3547 603-862-2053 603-862-0232 fax

## *University Actions*

On Friday, July 27<sup>th</sup>, 2007, a staff member recognized that information identifying a number of individual students had been included in this file. That individual notified the posting office, and the file was removed by the next work day. However, we subsequently learned on Thursday, August 9<sup>th</sup>, that a cached copy of the file was retained by the Google search engine. Through a request from UNH to Google, the cache was updated to remove the file on or about Sunday, August 12<sup>th</sup>.

An ongoing review of other popular search engines revealed only one other reference to this file. This was reflected by an outdated link to the original file on Yahoo! that displayed the name and social security number of a single student. UNH contacted Yahoo! and requested assistance in removing this link and that has occurred. Beyond this, we can find no further references to this file on the web.

The University's technical staff were able to collect some information about access to the original file that was posted to the UNH website. It appears that access to the original file came primarily from within UNH, presumably from UNH staff who accessed the credit hour and tuition data in the file as part of their work-related responsibilities. We have no evidence to suggest that this file was accessed by anyone with malicious intentions; however, because there has been some access from outside the university (and because we have no way of assessing access to the cached Google file), we can't offer you absolute assurances on this point.

For this reason, the University has arranged for a credit monitoring service to assist you with monitoring your accounts for the coming year. Naturally, the University will cover the full cost of this service.

We have partnered with ConsumerInfo.com®, an Experian® company, to provide you with a full year of credit monitoring. This credit monitoring membership will enable you to identify possible fraudulent use of your information.

Your credit monitoring product, Triple Alert<sup>SM</sup>, will identify and notify you of key changes that may be a sign of Identity Theft. Your complimentary membership includes:

- Monitoring of all three of your national credit reports every day
- Email alerts of key changes to any of your 3 national credit reports
- \$10,000 identity theft insurance provided by Virginia Surety Company, Inc.\*
- Dedicated fraud resolution representatives available for victims of identity theft

\*Due to New York state law restrictions, coverage cannot be offered to residents of New York.

You have ninety (90) days to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership quickly. To initiate your Triple Alert membership, please visit [insert URL] and enter the code provided below. You will be instructed on how to initiate your online membership.

Your Credit Monitoring Activation Code: [insert activation code]

### ***Additional Steps You Might Take***

In addition to the university's actions described above, we suggest that you consider contacting the three major credit reporting services to initiate one or both of the following steps:

1. Credit fraud alert—by placing a credit fraud alert on your consumer credit file, you will let creditors know to watch for unusual, suspicious activity related to your accounts.
2. Credit security freeze—by placing a credit security freeze, you prevent review of your credit history by creditors, insurance companies, and employers unless you give explicit permission for them to see your credit history.

(This information is drawn from the Federal Trade Commission's website on identity theft, located at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.)

Should you choose to pursue either (or both) of these strategies, the following contact information will facilitate your communication with the three major credit bureaus.

**Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 2002, Allen, TX 75013

**TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

**To limit the potential for your privacy to be placed at further risk, please be aware that no representative of the University of New Hampshire will contact you to request personal information related to this incident. If anyone makes such an attempt, please do not divulge any information. Contact us immediately at the number provided below to alert us to the possible fraud attempt.**

The University of New Hampshire is very serious about its responsibility to protect your personal information. This incident is an exception caused by human error and we are

truly sorry that it has occurred. If you would like to discuss this matter further, please feel free to contact me directly at (603) 862-2053.

Sincerely,

Mark Rubinstein  
Vice President for Student & Academic Services