



# UNIVERSITY of NEW HAMPSHIRE

November 30, 2011

Attorney General Michael Delany  
New Hampshire Department of Justice  
Office of the Attorney General  
33 Capitol St  
Concord, NH 03301


Re: Notification of Security Breach

Dear Attorney General Michael Delany:

I am writing to inform you of a recent security incident at the University of New Hampshire, located in Durham, New Hampshire.

We have reason to believe that a computer containing the name and social security number of one alumnus, and name and credit card information of another alumnus of the University of New Hampshire could have been accessed by an unauthorized outside party when an employee discovered a virus on their computer. Although we believe the exposure to be minimal, it is possible that the information of two alumni was accessed. We have removed the files from the hard drive of the compromised computer so that the files may no longer be found, have fully removed the virus from the computer, and are working with our IT department to minimize the risk of possible future incidents.

We notified the two affected persons on November 18, 2011, a copy of which is enclosed.

Sincerely,  


Peter Weiler  
President, UNH Foundation Inc.  
Elliot Alumni Center  
9 Edgewood Road  
Durham, NH 03824

Enc.



# UNIVERSITY of NEW HAMPSHIRE

November 17, 2011

<Salutation> <First><Last>

<Address 1>

<Address 2>

<City><State><Zip>

Dear <First>,

The purpose of this letter is to notify you that your personal information may have been inadvertently exposed to unauthorized access for a period of time after a University of New Hampshire employee's computer storing that information was breeched; we are not able to tell whether or not it was in fact accessed. The University deeply regrets this possible unauthorized access to 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 response to this incident. Additionally, although we have no way to know whether your data was accessed for purposes of misuse, we will be providing you with two years of a credit monitoring service through Experian if you chose to enroll. I will also offer some suggestions about other steps you might want to take to further protect yourself. Finally, I will provide contact information for follow up communication on this issue.

### ***Background: What Happened and University Actions***

One of our employees reported that on 10/20/2011 their computer exhibited unusual behavior, the desktop went blank and displayed error messages about the hard drive failing. The employee immediately turned off the computer and reported the problem and IT staff analyzed the machine. The machine was found to have malware.

As part of the response and due diligence, the machine was scanned for sensitive information and the scan indicated that your credit card information was present on the computer. While we do not know whether or not this event exposed your credit card information to unauthorized persons, as a courtesy and precaution we are contacting you to alert you to the situation and to offer you credit protection.

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

We have partnered with ProtectMyID from Experian to provide you with two full years of credit monitoring. This credit monitoring membership will enable you to identify possible fraudulent use of your information.

Your credit monitoring product, ProtectMyID, will identify and notify you of key changes that may be a sign of Identity Theft. Your complimentary membership includes:

- A free copy of your Experian credit report
- Daily monitoring and timely alerts of any key changes to your credit reports—so you know when there is any activity that you should be made aware of such as notification of new inquiries, newly opened accounts, delinquencies, public records or address changes
- Daily scanning of the internet of your social security, credit card, and debit card information to better protect you from potential fraud
- Monitoring of your address changes to minimize the threat of mail fraud
- Assistance with cancellation of your credit and debit cards
- Toll-free access to a dedicated team of fraud resolution representatives who will help you investigate each incident; contact credit grantors to dispute charges, close accounts if necessary, and compile documents; and contact all relevant government agencies
- \$1 Million Insurance policy- if you become a victim of identity theft while a member, you may be reimbursed up to \$1 million for costs such as lost wages, private investigator fees, and unauthorized electronic fund transfers.\*

You have until February 29, 2012 – date to be supplied by Experian – to activate this protection. We encourage you to activate your credit monitoring membership quickly. To initiate your Triple Alert membership, please visit <http://www.protectmyid.com/enroll> and enter the code provided below. You will be instructed on how to initiate your online membership. If you prefer, you can enroll on the phone by speaking with Experian Customer Care representatives toll-free at (877) 441-6943.

Your Credit Monitoring Activation Code: <insert code here>

As soon as you enroll in your complimentary ProtectMyID membership, Experian will begin to monitor your credit reports from Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup> on a daily basis and notify you of key changes. This powerful tool will help you identify potentially fraudulent use of your information, and provide you with immediate assistance from a dedicated team of fraud resolution representatives should you ever need help.

### ***Other possible precautions***

If you feel that the information about you that is listed above could give someone inappropriate access to your financial services, you might 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. The cause of this incident is under investigation. We are truly sorry that it has occurred.

Sincerely,

Peter Weiler  
President, UNH Foundation Inc.  
Elliot Alumni Center  
9 Edgewood Road  
Durham, NH 03824