



OFFICE OF UNIVERSITY COUNSEL

Martin A. Oppenheimer
Senior Counsel

July 7, 2011

Attorney General Michael A. Delaney
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

Pursuant to New Hampshire Rev. Stat. 359-C.20, we are writing to inform you that a laptop owned by Tufts was stolen, and that the laptop contained the Social Security numbers of 73 individuals, of whom 1 was a New Hampshire resident.

I. Nature of the unauthorized use or access

The laptop was used by a research associate who was working with one of our professors on research at Massachusetts General Hospital (MGH). The laptop was primarily used to store research data, but in early 2010, a spreadsheet containing information on a number of applicants to the Graduate School of Arts and Sciences at Tufts was downloaded to the computer and was never removed. Some of the applicants' Social Security Numbers were included in the file.

The theft occurred in late April, 2011. Because the research associate was employed at MGH, she notified their IT Department. She also filed a police report. When reporting the theft, the laptop user also reported that, although the computer was encrypted, she believed that it might not have been fully shut down when stolen, and so someone finding the laptop might have been able to access the data without a password.

On June 16, 2011, Tufts' Office of University Counsel first learned that University files containing personally identifiable information might have been compromised.

II. Number of New Hampshire residents affected

We have identified 1 New Hampshire resident whose personal information may have been exposed to third parties.

Notice to each of the affected individuals that we have thus far identified is being mailed on or about July 8, 2011. A copy of the notice is enclosed. As noted in the letter to affected individuals, we also are offering each affected person one year of free credit monitoring from Experian, a recognized credit monitoring provider.

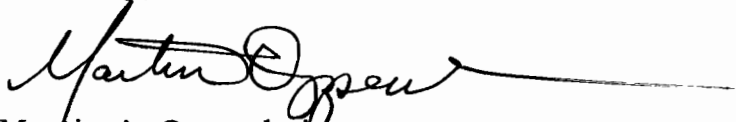
III. Steps we have taken or plan to take relating to the incident

The file in question dates back to the spring of 2010. Since that time, Tufts has implemented a Written Information Security Program, appointing information stewards for each of the schools throughout the university and requiring users to take steps to (i) identify where personal information is being stored, (ii) securely destroy information that is no longer needed, and (iii) maintain adequate security safeguards for personal information. We have been advised by the admissions office of the Graduate School that applicants' Social Security numbers are no longer distributed to faculty members as part of the admissions process.

IV. Contact Information

We trust that this letter and its enclosures provide you with all the information required to assess this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Martin Oppenheimer", with a long horizontal flourish extending to the right.

Martin A. Oppenheimer
Senior Counsel for Business Affairs

July xx, 2011

<name1>
<line1>
<line2>
<line3>
<line4>
<line5>

Dear <salutation> <name1>,

Tufts University and the Graduate School of Arts and Sciences take very seriously their obligation to protect the personal information of students and other members of our community. We have instituted policies to contain and control the use of personal information and have conducted university-wide programs to eliminate sensitive information from individual computers. Thus, we deeply regret any situation where such information may be put at risk.

We recently learned of an apparent breach in security on a stolen laptop owned by Tufts. While the theft was reported to the police, the computer has not been found.

We are letting you know because one of the files on the computer apparently contained information on candidates for admission to the graduate program in the Department of Psychology in early 2010. Unfortunately, this file included your name and Social Security number, as well as contact and educational information such as your grade point average (GPA) and Graduate Record Examination (GRE) score. While the data was encrypted, the laptop user was uncertain if the computer had been properly shut down at the time it was stolen.

There is no direct evidence of unauthorized use of personal information. However, as a precaution, Tufts is notifying all those affected by the breach and has arranged for Experian, a third party, to provide a year of free credit monitoring to any affected individuals who elect to use it. In order to activate your credit monitoring, please visit <http://partner.consumerinfo.com/triple> and click on "Start Your Complimentary Membership Here." You will be asked to enter your information, and a special activation code, which is <CREDIT REPORTING CODE>. Also enclosed is additional information on what you can do if you believe your identity has been stolen.

Please accept our sincere apologies for any inconvenience or concern this may cause. If you should have any further questions, please contact us Monday-Friday 9:00 a.m. to 5:00 p.m. ET at 1-617-627-3269. Thank you.

Sincerely,

Lynne Pepall, Dean
Graduate School of Arts and Sciences

Enclosure

ADDITIONAL INFORMATION FOR AFFECTED INDIVIDUALS

If my name was on a breached computer, does that mean I am the victim of identity theft?

No. The fact that someone may have had access to your information does not mean that you are a victim of identity theft. The university has no direct evidence of unauthorized use of personal information. As a precaution, Tufts is notifying all those affected by the breach and has arranged for Experian, a third party, to provide a year of free credit monitoring to any affected individuals who elect to use it.

What do I do if I am a victim of identity theft?

You should immediately report the crime to your local law enforcement agency, contact any creditors involved, and notify the credit bureaus.

If you are a Massachusetts resident, detailed information is available on the identity theft victim page on the website of the Massachusetts Office of Consumer Affairs and Business Regulation: <http://www.mass.gov/ocabr>. Additional information can also be found at the Identity Theft Resource Center: <http://www.idtheftcenter.org>.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

If you live in Iowa, report any suspected identity theft to law enforcement or the Attorney General of Iowa.

If you live in Oregon, report any suspected identity theft to law enforcement or the Federal Trade Commission at the contact information below.

If you live in Maryland or North Carolina, you can obtain information about the steps you can take to avoid identity theft from the Maryland and North Carolina Offices of Attorneys General and the Federal Trade Commission.

Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	North Carolina Office of the Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com	Federal Trade Commission Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/bcp/edu/microsites/idtheft
---	--	--

What is a fraud alert, and how do I go about placing it on my credit file?

A fraud alert is a no-cost service intended to prevent other people from fraudulently receiving credit in your name. Most credit card companies and other creditors will not issue credit without first checking the applicant's credit report. A fraud alert tells credit issuers that there is possible fraud associated with the account and gives them a phone number to call before issuing new credit in your name. When you call the credit bureau fraud line, you will be asked for identifying information and will be given an opportunity to enter a phone number for creditors to call.

In order to place a no-cost fraud alert on your consumer credit file, you should contact one of the three national credit bureaus. Once a credit bureau places a fraud alert on your credit file, the two other credit bureaus will automatically do the same; however, you may want to contact each bureau directly. Here is the contact information for the fraud divisions of the national credit bureaus:

- **Equifax:** (888) 766-0008 or www.equifax.com
- **Experian:** (888) 397-3742 or www.experian.com
- **TransUnion:** (800) 680-7289 or www.transunion.com

The credit bureaus will send you a confirmation letter indicating that you have placed a fraud alert on your consumer credit file. An initial fraud alert lasts 90 days; you may reinstate it after that.

How do I order my free credit report?

Once you've placed a fraud alert on your consumer credit file, the credit bureaus will send you confirmation letters, which will contain instructions on how to obtain a free credit report.

If you will not be placing a fraud alert, you may still obtain a copy of your credit report, free of charge. We recommend that you remain vigilant and review your free credit reports and account statements for any unauthorized or suspicious activity. You may obtain a free copy of your credit report by contacting any one or more of the following agencies:

Equifax P.O. Box 740241 Atlanta, Georgia 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-888-4213 www.transunion.com
---	--	--

What should I look for in my credit report?

In your credit report, be alert for any suspicious activity. Look especially for any accounts you did not open and any charges you did not make. Look at the inquiries or requests section for names of creditors from whom you have not requested credit. Look in the personal information section to confirm the accuracy of addresses where you have lived and your Social Security number. Any suspicious activity in these areas may be indications of fraud. Also, be on alert for calls from creditors or debt collectors about bills that you do not recognize and for unusual charges on your credit card bills.

What is a security freeze, and how do I go about activating it?

Massachusetts law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing a security freeze on your credit report may delay, interfere with, or prevent timely approval of requests you make for new loans, credit mortgages, employment, housing, or other services; therefore, take time to consider the benefits and potential drawbacks of a security freeze.

If you have been a victim of identity theft, the agency cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a \$5 fee to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed below by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion Security Freeze (FVAD) P.O. Box 6790 Fullerton, CA 92834-6790 1-800-680-7289 www.transunion.com
---	--	--

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Proof of current address such as a current utility bill or telephone bill
3. Date of birth
4. Social Security number
5. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)
6. If you have moved in the past five years, provide the addresses where you have lived over the prior five years.
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

After receiving your request, the credit bureaus have three business days to place a security freeze on your credit report. The bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze entirely, send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

What is the difference between a fraud alert and a security freeze?

A fraud alert is a special message on the credit report that a credit issuer receives when checking a consumer's credit rating. It tells the credit issuer that there may be fraud involved in the account. Most businesses will not open credit accounts without first checking a consumer's credit history. A security freeze means that your credit file cannot be seen by potential creditors, insurance companies, or employers doing background checks unless you give your consent.

Will credit monitoring, fraud alert, or a security freeze prevent me from using my credit cards or getting new ones?

None of these services will stop you from using your existing credit cards or other accounts. A fraud alert may slow the process of receiving new credit, since the purpose of a fraud alert is to help protect you against an

identity thief opening credit accounts in your name. Potential creditors receive a special message alerting them to the possibility of fraud, and they know that they should re-verify the identity of a person applying for credit. With a security freeze, potential creditors, insurance companies, or employers doing background checks are not permitted to see your credit history. Among other things, this would likely prevent you from receiving new credit without your explicit consent.

Is it OK to give my Social Security number to the credit bureau fraud line?

The credit bureaus ask for your Social Security number and other information in order to identify you and avoid sending your credit report to the wrong person. However, Tufts advises caution if you are contacted by somebody who claims to represent Tufts on this matter and who asks for personal information. The university will not contact you and ask for your full Social Security number, bank account, or other personal information.

What is credit monitoring?

Credit monitoring is a service that continuously monitors your credit reports at the three major credit bureaus and alerts you of any suspicious activity or changes to your reports, such as employment changes, changes to current accounts, address changes, credit inquiries, or new accounts. In order to activate your credit monitoring through Experian, please follow the directions provided in your notification letter from Tufts.

What if the credit monitoring service detects a problem?

If you receive a report of suspicious activity, call Experian at the telephone number listed below and review the report with a member of the staff. If information in the credit report cannot be explained, you may wish to file a report of suspected identity theft with your local police or sheriff's department, and obtain a copy of it. You may also elect to place a fraud alert on your consumer credit file if you have not already done so.

Whom can I call if I have further questions?

If you should have any further questions, please contact us at 617-627-3269.