



JOHN ELIAS BALDACCI  
GOVERNOR

STATE OF MAINE  
DEPARTMENT OF PROFESSIONAL  
AND FINANCIAL REGULATION  
BUREAU OF CONSUMER CREDIT PROTECTION  
35 STATE HOUSE STATION  
AUGUSTA, MAINE  
04333-0035

WILLIAM N. LUND  
SUPERINTENDENT

**MEMORANDUM**

TO: ✓ Linda Conti, Assistant Attorney General  
Office of the Attorney General  
6 State House Station  
Augusta, ME 04333-0006

cc: Martin A. Oppenheimer, Esq.  
Senior Counsel for Business Affairs  
Tufts University  
Ballou Hall  
Medford, MA 02155

FROM: William N. Lund, Superintendent  
Bureau of Consumer Credit Protection

RE: Notification of File Breach; Tufts University

DATE: June 16, 2010

CONSUMER PROTECTION DIVISION  
**RECEIVED**  
JUN 21 2010  
OFFICE OF ATTORNEY GENERAL

Enclosed please find letters dated May 21, 2010 and June 3, 2010 from the Senior Counsel of Tufts University describing a file breach that was discovered in February, March and April, 2010.

I have spoken with Tuft's counsel, Martin Oppenheimer, and in my opinion he has satisfactorily completed the university's notification requirements pursuant to 10 MRSA §1348. I told him I would forward those materials to you, since your office is the appropriate recipient of this information because Tufts is not a financial services provider subject to regulatory oversight by any bureaus or offices within this Department.

Please let me know if you have any questions.

Thank you.

Enclosures



PRINTED ON RECYCLED PAPER

OFFICES LOCATED AT: 76 NORTHERN AVENUE, GARDINER, MAINE 04345

PHONE: (207) 624-8527 (Voice)

TTY (for Hearing Impaired): 1-888-577-6690

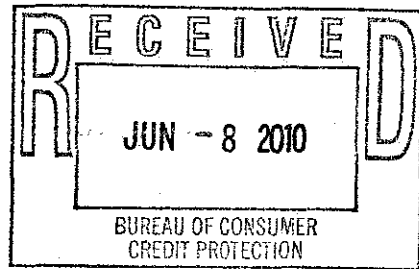
INTERNET: [www.Credit.Maine.gov](http://www.Credit.Maine.gov)

FAX: (207) 582-7699



OFFICE OF UNIVERSITY COUNSEL

Martin A. Oppenheimer  
Senior Counsel



May 21, 2010

Commissioner Anne L. Head  
Department of Professional and Financial Regulation  
35 State House Station  
Augusta, ME 04333

**Re: Notification of Security Breach**

Dear Commissioner Head:

Pursuant to Maine Statute Title 10 § 1348, we are writing to inform you that several computers on our network were exposed to malware and that, based on our current review, may have resulted in an unauthorized acquisition of personal information. Tufts University takes this very seriously and is in the process of performing a careful analysis to determine the overall extent of this incident.

**I. Nature of the unauthorized use or access**

We have determined that certain users were unknowingly infected with the "torpig" malware, which may have allowed a third party access to stored data on Tufts computers. The first two such incidents came to our attention on February 18, 2010. Additional incidents came to our attention on March 9, March 16 and April 2. Because of the similarity of the malware, we are treating the incursion as one multi-faceted incident. The forensic analysis of the various computers by the outside consultant retained by Tufts was completed on May 7, 2010.

The attacks involved malicious advertisements that were placed on remote websites; upon visiting the website the Tufts computers were scanned and vulnerabilities were exploited, allowing the attackers to install and run malware without requiring any input or clicking on the part of the Tufts user. The malware, classified as a variant of 'torpig', was designed to search the computer for personal information and then upload it to remote command and control servers, in addition to providing the remote attacker the ability to install and execute arbitrary software on the compromised computer.

All of the personal information involved was in electronic form, and all were Social Security numbers. (Until 2004, Tufts used students' Social Security Numbers as their university identification number, so older records would contain this number even if no health or financial information was involved.)

## **II. Number of Maine residents affected**

We have thus far identified 27 Maine residents whose personal information may have been exposed to third parties. One additional computer was compromised but our forensic consultant, after extensive testing, informed us on May 11, 2010 that it could not reach a definitive opinion as to whether or not personal information was accessed. To be cautious, we have decided to notify the individuals whose information was on that computer, and are in the process of gathering those individuals' addresses.

Notice to each of the affected individuals that we have thus far identified is being mailed on Monday, May 24, 2010. 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**

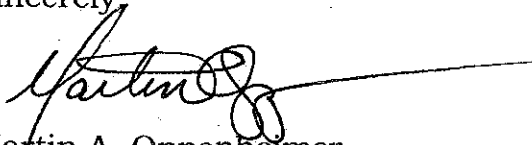
Upon learning of the first incident, Tufts arranged for an internal forensic review of the hard drives, as well as several days of netflow, anti-virus and IDS log messages. The computers in question were promptly isolated so that no further access was possible. Tufts also engaged an outside contractor, cmd Labs of Baltimore, MD, to assist in the analysis. Cmd Labs' three principals are recognized experts in the field of digital forensics and cyber-crime investigation.

Tufts has diligently updated anti-virus definitions to improve detection of this class of malware, and has deployed security patches from software vendors to mitigate the risk going forward. Additionally, schools and departments across the University are implementing provisions from our Written Information Security Program, including (i) identifying where personal information is being stored, (ii) securely destroying information that is no longer needed, and (iii) reviewing the security safeguards in place for personal information that does need to be maintained, to ensure that such safeguards meet the requirements outlined within 201 CMR 17.00.

#### **IV. Contact Information**

We trust that this letter and its enclosures provide you with all the information required to assess this matter. For any additional information, please contact me by phone at (617) 627-3337 or by email at [martin.oppenheimer@tufts.edu](mailto:martin.oppenheimer@tufts.edu). Thank you.

Sincerely,

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

Martin A. Oppenheimer  
Senior Counsel for Business Affairs

May XX, 2010

<name1>  
<line1>  
<line2>  
<line3>  
<line4>  
<line5>  
<line6>

Dear <salutation>,

As a precautionary measure, we are writing to inform you of an apparent breach in security on a computer in the Athletics Department at Tufts University. Recently, Tufts discovered that this computer—and a small number of unrelated computers—had been exposed to malicious software, or malware. Malware searches computers for sensitive personal information, and can be downloaded to a computer when the user visits a seemingly safe site. Even though Tufts makes antivirus software available for all of its computers, it may take time before a new version of malware is identified and addressed by the protective software.

Unfortunately, one of the files on the computer contained your name and Social Security number. While there is 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. 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.

Over the last five years, Tufts has instituted policies to contain and control use of personal information, such as Social Security numbers. The official university database of record for all alumni does not contain such sensitive information. [In line with data privacy regulations recently enacted in Massachusetts and elsewhere, an aggressive university-wide effort is underway to locate and protect or securely destroy sensitive information maintained by the university.]

Please accept our apologies for any inconvenience or concern this may cause. If you should have any further questions, please contact our information line, which is in operation Monday-Friday 9:00 a.m. to 5:00 p.m. ET at 1-877-566-1788 (toll-free) or 1-617-627-1700.

Sincerely,

<Scott signature 4-28-10\_black.tif>

Scott G. Sahagian  
Executive Associate Dean  
Tufts School of Engineering

<L.McIntosh Sig.tif>

Leah McIntosh  
Executive Administrative Dean  
School of Arts and Sciences

**ADDITIONAL INFORMATION FOR AFFECTED INDIVIDUALS**

**If my name was on a breached computer, does that mean I am the victim of identify 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.

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

**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](http://www.equifax.com)
- Experian: (888) 397-3742 or [www.experian.com](http://www.experian.com)
- TransUnion: (800) 680-7289 or [www.transunion.com](http://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<br>P.O. Box 740241<br>Atlanta, Georgia<br>30374<br>1-800-685-1111<br><a href="http://www.equifax.com">www.equifax.com</a> | Experian<br>P.O. Box 2002<br>Allen, TX 75013<br>1-888-397-3742<br><a href="http://www.experian.com">www.experian.com</a> | TransUnion<br>P.O. Box 2000<br>Chester, PA 19022<br>1-800-888-4213<br><a href="http://www.transunion.com">www.transunion.com</a> |
|---|--|--|

**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<br>P.O. Box 105788<br>Atlanta, GA 30348<br>1-800-685-1111<br><a href="http://www.equifax.com">www.equifax.com</a> | Experian Security Freeze<br>P.O. Box 9554<br>Allen, TX 75013<br>1-888-397-3742<br><a href="http://www.experian.com">www.experian.com</a> | TransUnion Security Freeze (FVAD)<br>P.O. Box 6790<br>Fullerton, CA 92834-6790<br>1-800-680-7289<br><a href="http://www.transunion.com">www.transunion.com</a> |
|---|--|--|

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 our information line by phone at 1-877-566-1788 or 617-627-1700.