

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: The University of North Carolina at Greensboro (UNCG)

Address: 1400 Spring Garden Street, Greensboro, NC 27412

Telephone: 336-334-5266

Fax: _____

Email: caonel@uncg.edu

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: 16 December 2008

Date the Security Breach was discovered: 11 December 2008

Estimated number of affected individuals: 2500

Estimated number of NC residents affected: 2500

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): UNCG

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: A malware virus was discovered on a computer in our Payroll and Accounting Services Department. The computer that contained social security numbers, and bank account and bank routing numbers for payroll direct deposits for all UNCG employees

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: Password protection, virus detection with frequent updates.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: When the security breach was discovered, UNCG technicians made a copy of the data on the affected workstation. They took the workstation offline, so the virus which had been detected could not access the network. The hard disk of the affected workstation was reformatted. The workstation was reloaded with a clean copy of the operating system, and best practices were used to ensure that this image was protected, the most current virus protection programs were loaded, and the most current virus protection pattern file was in use.

Date affected NC residents were/will be notified: 15 December 2008

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): NA

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?
(pursuant to N.C.G.S. § 75-65(e))

- written notice
 electronic notice (email)
 telephone notice
 substitute notice

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Signature: /Lucien Capone III/ Date: 16
December 2008

Contact Person, Title: University Counsel

Address: 307 Mossman Building, UNCG, Greensboro, NC
27412

(if different from above)

Telephone: 336-334-3067 Fax: 336-256-0531

Email: caponel@uncg.edu

December 15, 2008

To: Faculty, Staff and Student Employees

From: Reade Taylor
Vice Chancellor for Business Affairs

Re: Security Breach Involving Personal Information - URGENT

I am writing to inform you there has been a security breach of a university's Accounting Services computer that contains personal information of our employees, including social security numbers and direct deposit bank routing and account numbers. A virus may have allowed an unauthorized person to gain access to your information. We have been unable to determine whether or not any information has actually been accessed by unauthorized persons. Because the consequences of such access are potentially serious, we believe it is prudent to provide you with this notification and to advise you to monitor your account to which direct deposits from the university are made.

When the security breach was discovered, UNCG technicians made a copy of the data on the affected workstation. They took the workstation offline, so the virus which had been detected could not access the network. The hard disk of the affected workstation was reformatted. The workstation was reloaded with a clean copy of the operating system, and best practices were used to ensure that this image was protected, the most current virus protection programs were loaded, and the most current virus protection pattern file was in use.

In addition to the steps we have taken to protect your information from future unauthorized access, we will provide notification to the three major credit reporting agencies - TransUnion, Experian, and Equifax - and the Consumer Protection Division of the North Carolina Attorney General's office.

We advise you to check your direct deposit account to ensure no unauthorized activities have occurred. You should: 1) check to verify that no fraud has occurred, and 2) monitor your accounts, because stolen data could be used for future fraud. **The December payroll is already in transit to employees' designated bank accounts. Therefore, should you desire to close your existing account, it is imperative you do not do so until you have verified your December deposit has been credited to it.** You may also wish to check your credit report. You are entitled to one free credit check per year per

credit reporting agency, and you may access that report by visiting the following web site: <https://www.annualcreditreport.com/cra/index.jsp>

If you suspect any fraudulent activity on your account, we suggest that you place a *free* "fraud alert" on your personal credit file if you have been victimized or believe you could become a victim of identity theft. A fraud alert tells creditors to either contact you or use reasonable policies and procedures to verify the consumer's identity before they open any new accounts in your name or change your existing accounts. To place a fraud alert on your file, you should call any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax
1-877-576-5734

Experian
888-397-3742

TransUnion
800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. The Fair and Accurate Credit Transaction Act of 2003 (or FACT Act) gives all consumers the ability to obtain an annual credit report from each of the three credit bureaus *free of charge*. If you find any information relating to fraudulent transactions, you should contact the credit bureau to determine how to have the transaction deleted.

The FTC also provides helpful information about identity theft. For more information, go to www.ftc.gov and click on "Information on Free Credit Reports" or call the FTC hotline at 1-877-IDTHEFT. If you believe you have been a victim of identity theft, we encourage you to contact the FTC immediately by calling the FTC hotline or at www.ftc.gov/idtheft.

Please accept our apologies for this situation. We take our responsibilities for safeguarding your financial and personal information very seriously. In closing I want to emphasize this was a security breach with potential data loss. While we understand that this may not alleviate all of your concerns, be assured that UNCG is taking the appropriate steps to review and enhance our security protocols.

If you have questions, you may call 336-334-5851, Monday through Friday from 9 a.m. to 5 p.m. or visit the following web site: <http://fsv.uncg.edu/incident/>