NORTH CAROLINA COMMUNITY COLLEGE SYSTEM

R. Scott Ralls, Ph.D.
President

December 16, 2009

SUPERSEDES SELECT NUMBERED MEMO S09-001

MEMORANDUM

TO: Presidents
Business Officers
Library Directors
Registrars
System and Network Administrators

FROM: Saundra W. Williams, Senior Vice President
Technology and Workforce Development

SUBJECT: Library Server Security Breach

The purpose of this memo is 1) to inform you of an information security breach that involves your college; 2) to inform you of the corrective actions that have taken place to remedy the current breach; 3) to inform you of the actions that have taken place to prevent future incidents of this type; and 4) to inform you of the actions required from you and your college.

On August 23, 2009, the System Office experienced a compromise of its production Sirsi library server. The library server provides a data entry system for cataloging and tracking library materials for 46 community college libraries. The server is accessed by 270,000+ patrons.

The system was accessed by unauthorized users. The attempt was discovered the next morning, August 24, 2009, by the server administrator while performing daily administrative tasks. Steps were taken immediately following the incident to remedy the issue. At this time, it appears that the compromise was limited to the operating system and the installation of “chat” software. There is no evidence that any data was accessed. The data is stored in an obscure database which the unauthorized user would have to know the structure of the database to piece the information together to match the person’s name with other personally identifiable information (PII). Examples of PII are Social Security Numbers and Driver’s Licenses. As required by the State’s Information Technology Services (ITS); an incident report was submitted to ITS.

CC09-045
E-Mail

Corrective Actions

Once the ticket was submitted, ITS reviewed the history and consulted with the Attorney General's Office. Although it does not appear the data was accessed, the Attorney General's recommendation is that it must be treated as such. Since some driver's licenses were contained on the server, the AG stated that we are to follow the General Statutes: G.S. 132-1.10(c1) & G.S. 75-65 for notifying the patrons.

On December 5, 2005, the CCLINC Steering Committee recommended that all colleges be required to remove all Social Security Numbers from the server to comply with the North Carolina Identity Theft and Protection Act. The Steering Committee passed the recommendation and was noted in the minutes of the December 6, 2005 meeting which was communicated to the 46 participating colleges. On page four of the minutes, the Steering Committee approved 1) that the use of Social Security Numbers be stopped and 2) the Social Security Numbers are removed by July 1, 2007. At the time the action did not address Driver's Licenses and the General Counsel at the System Office approved the colleges to continue to collect the Driver's Licenses. Since 2005, Driver's Licenses have been added as protected information. There were 19 colleges that stored approximately 9000 patrons' Driver's Licenses in the database.

Therefore, the 9,000 patrons must be notified in writing of the incident. On behalf of the impacted colleges, t he System Office will take on the responsibility of notifying the all patrons and bear the associated mailing costs. The System Office will also address any inquiries from the patrons regarding the incident.

The CCLINC Steering Committee has subsequently approved a policy prohibiting the storage and collection of Driver's Licenses, State identification cards, or passport numbers. All Social Security Numbers and Drivers' Licenses must be removed from the system by Monday, January 4, 2010. Each college is responsible for ensuring that this information is removed and no longer collected.

Additionally, the System Office's Information Services Group has taken corrective actions to prevent further unauthorized access to the server and continues to monitor the server for malicious activity.

The System Office will also conduct periodic reviews of the database to ensure that no personally identifiable information is being stored.

Additional Findings

As the System Office has reviewed the data stored on the library server, approximately 42,500 Social Security Numbers were found in use by 12 colleges. To be consistent with the policy approved by the CCLINC Steering Committee in December 2005 and to be consistent with the General Assembly's intent in G.S. 132-1.10(a), colleges should remove all social security numbers stored on the library server.

CC09-045
E-mail

A conference call with the Library Directors of the 12 affected colleges was held on Monday, November 23, 2009. This call was used to communicate background information, next steps, and answer any questions. The 12 affected colleges required to attend this meeting were notified directly by the System Office via phone.

Actions Required by Your College

In order to notify all patrons with Driver's License or Social Security Numbers that were stored in the Patron Database, the System Office will mail the notification letters out on or about **Monday, December 23**. The letter to be mailed is attached for your information.

Each of the 12 CCLINC College Presidents that are affected must acknowledge this notification and certify that their college will notify their patrons. The System Office will send these 12 Presidents and their Library Directors the certification letter separately. Certification letters can be faxed to (919) 807-7164.

Attached you will find a copy of the letter that will be mailed to all affected library patrons.

If you have any questions, please contact Jason Godfrey at (919) 807-7054 or godfreyj@nccommunitycolleges.edu.

Thank you for your cooperation and assistance in this matter.

SWW\jcg/dcm

Attachment

c: Dr. R. Scott Ralls
Mr. Kennon Briggs
Ms. Q. Shanté Martin
Ms. Ruth Bryan
Mr. Jason Godfrey

CC09-045
E-mail

NORTH CAROLINA COMMUNITY COLLEGE SYSTEM
Dr. R. Scott Ralls, President

December 17, 2009

[NAME]
[Mailing address]
[City], [State] [ZIP]

Dear Community College Library Patron,

On behalf of [COLLEGE NAME], we are writing to inform you that the North Carolina Community College System suffered a security breach caused by unauthorized access to a computer server that hosts library patron information. We are sending this notification, in accordance with Article 2A of Chapter 75 of the North Carolina General Statutes, (N.C.G.S. § 75-65) which governs identity theft, to report that your [SOCIAL SECURITY NUMBER/DRIVER'S LICENSE NUMBER/SSN & DL] was stored in a database on the server. Our investigation indicates that the computer hacker only accessed the operating system and none of your personal data was compromised. Further, we have no evidence that personally identifiable information, as defined by law, was retrieved from the library database.

We have reviewed our current policies and procedures and have revised them to mitigate further access by unauthorized users to our servers. We also are purging information that the law defines as personally identifiable from the library server. In addition, North Carolina community colleges no longer collect or store library patrons' personally identifiable information, as defined by law, and strive to protect the personal information of our constituents. On the back of this letter, you will find more information from the N.C. Attorney General's Office on what to do if you receive a letter about a security breach.

We regret that this situation occurred, and we apologize for any inconvenience to you. If you have further questions, please call (919) 807-7241 or e-mail LibraryInfo@nccommunitycolleges.edu.

Sincerely,

Dr. Saundra W. Williams
Senior Vice President and Chief of Technology and Workforce Development

From NC Attorney General's Web site:
http://www.ncdoj.com/Help-for-Victims/ID-Theft-Victims/Received-a-Security-Breach-Letter.aspx

Received a Security Breach Letter?

Under North Carolina law, businesses and state and local government agencies must let you know if your personal information has been compromised by a security breach.

They must also report security breaches to the Attorney General's Office. A total of 329 breaches that involved information of nearly 1.7 million North Carolina consumers have been reported to our office since 2005.

What is a Security Breach?

A security breach happens when data or records containing personal information, such as Social Security numbers, bank account numbers or driver's license numbers are lost, stolen or accessed improperly. This kind of information can be used by criminals to commit identity theft.

Being notified that your information was part of a security breach does not necessarily mean you'll become a victim of identity theft. However, you are at a greater risk and need to take steps to protect yourself.

Step 1: Sign Up for Free Services

Some businesses or government agencies offer security breach victims a free service such as credit monitoring. While most offers are genuine, don't provide private information without verifying that the credit monitoring service is legitimate.

Step 2: Notify the Credit Bureaus

Request a fraud alert from one of the credit bureaus. This tells banks and other creditors to take extra steps to verify your identity before issuing credit in your name. A fraud alert is free and will last 90 days unless you request an extended seven-year fraud alert and provide a police report. You'll also get a free copy of your credit report, which you should review carefully.

To request a fraud alert, contact one of the three nationwide credit bureaus.

Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

Step 3: Consider a Security Freeze

A security freeze stops access to new credit in your name. Placing a security freeze prohibits credit reporting agencies from releasing any information about you to new creditors without your approval, making it difficult for an identity thief to use your information to open an account or obtain credit.

North Carolina consumers can now get free security freezes online. Identity theft victims who have filed a police report, their spouses, and consumers over the age of 62 can also get free security freezes by mail or phone. Other consumers can get security freezes by mail or phone for a fee.

Step 4: Monitor Your Credit

Continue to review your credit reports every few months. Your private information that was released in the security breach may not be used right away. You can request a free credit report annually.

Notifying Law Enforcement

Most law enforcement will not issue you a police report until your private information is actually used by an ID thief. If you have any suspicion that your information is being used by a thief, contact local law enforcement immediately.