North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

OFFICE OF GENERAL COUNSEL
Campus Box 7008
Raleigh, NC 27695-7008

NC STATE UNIVERSITY

An Equal Opportunity/Affirmative Action Employer

919.515.3071 (main office)
919.515.3060 (fax)

STATE OF NH
DEPT OF JUSTICE
2016 JUL 14 AM 11:40

July 8, 2016

Office of the Attorney General - New Hampshire
33 Capitol Street
Concord, NH 03301

RE: Security Breach Notification

To Whom It May Concern:

On June 3, 2016 North Carolina State University (NC State) learned that a university employee's email account was illegally accessed by an unauthorized person. The breach was a result of the employee's credentials being compromised during a phishing attack.

While investigating the incident, NC State learned that the email account contained approximately 36,403 student names, social security numbers, and 2013 mailing addresses. In conjunction with law enforcement, NC State quickly initiated its incident response team, performed computer forensics, scanned the account for all possible data, developed the notification lists and retrieved credit monitoring codes for all potentially affected individuals. 35 New Hampshire residents were affected.

NC State was not able to determine if this unauthorized user retrieved or accessed this information. There is no evidence to suggest that an unauthorized person has retrieved or misused any personal identifying information in connection with this unauthorized access.

Pursuant to North Carolina General Statute § 75-65, NC State provided notifications of the breach to the affected individuals as quickly as feasible and without unreasonable delay. Working with law enforcement, NC State has been investigating the potential access of personal information and provided notice as quickly as possible to the relevant regulatory bodies and agencies and three major credit bureaus.

NC State provided notification to the affected individuals, posted notice on NC State's website, and notified media. Additionally, NC State has provided credit monitoring services to affected individuals.

Upon learning of this security incident, the university has taken aggressive steps to avoid future unauthorized access to personal information. NC State's actions included: (1) removing the file and email(s) containing personal identifying information from the compromised email account, (2) requiring affected university employees to change their account credentials and increase security protocols, including 2-Step Verification, and (3) requiring additional and focused information security protocols to be implemented within the affected unit as well as more broadly throughout campus to all systems containing sensitive data.

NC State is committed to protecting the information and data we maintain and will continue to monitor this situation. If you have any additional questions about this matter, please contact NC State's University Records Officer.

Sincerely,

Aubry A. Dix
University Records Officer

NC STATE UNIVERSITY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

On June 3, 2016 North Carolina State University (NC State) learned that a university email account was illegally accessed by an unauthorized person. The unauthorized access created the potential for the individual to view or have access to certain personal identifying information. You are receiving this notification because the email account which was accessed contained a file from 2013 which included your name, 2013 mailing address, student ID number, and social security number, and/or other email(s) which contained your name and social security number.

There is no evidence that any personal data has been retrieved or misused or that fraud has been committed using this information. Nevertheless, NC State is notifying you of the unauthorized access and informing you of measures that you can take to protect your identity. Being notified that your information was part of a security incident does not necessarily mean you will become a victim of identity theft. However, you could be at a greater risk for such theft.

To mitigate this risk NC State will be providing affected individuals with credit monitoring services for one year. Attached you will find instructions to access these services. The instructions include an activation code to participate in this credit monitoring service.

Upon learning of this security incident, the university has taken aggressive steps to avoid future unauthorized access to personal information. NC State's actions included: (1) removing the file and email(s) containing personal identifying information from the compromised email account, (2) requiring affected university employees to change their account credentials and increase security protocols, including 2-Step Verification, and (3) requiring additional and focused information security protocols to be implemented within the affected unit as well as more broadly throughout campus to all systems containing sensitive data.

In addition, we are notifying you of this unauthorized access so you can take action along with our efforts to minimize or eliminate potential harm. We also have advised the North Carolina Attorney General's Office and the following three major consumer reporting agencies: Equifax, Experian, and TransUnion.

NC State is committed to protecting sensitive and confidential information. Pursuant to the Fair Credit Reporting Act, you may request your credit report, which will be sent to you free of charge (www.annualcreditreport.com). You should remain vigilant by reviewing account statements and monitoring free credit reports. To place a fraud alert and/or security freeze on credit files, you may contact any one of these three major credit bureaus:

Equifax: 1-888-525-6285
www.equifax.com
P.O. Box 740256
Atlanta, GA 30374

Experian: 1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion: 1-800-680-7289
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

A fraud alert will notify creditors that before they issue new credit lines or credit cards, they must notify you to determine if the request is legitimate. A security freeze will prohibit the consumer reporting agency from releasing your credit report or any information to a third party, with limited exceptions, without your prior express authorization. If you find that you have been a victim of identity theft, you should notify your local law enforcement agency or the North Carolina Attorney General's Office. For more information about preventing identity theft, please contact the Federal Trade Commission or the North Carolina Attorney General's Office.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357
www.ftc.org

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
www.ncdoj.gov

In addition to the advice provided here, the North Carolina Attorney General's Office provides advice for people who are affected on their website: http://www.ncdoj.com/Help-for-Victims/ID-Theft-Victims/Security-Breach.aspx

We share your concerns and regret this situation. NC State is committed to protecting the information and data we maintain and will continue to monitor this situation. If you have any additional questions about this matter, please visit http://go.ncsu.edu/cashiers-office-notification or contact 1-844-787-6811 Monday through Friday, 9:00AM to 9:00PM Eastern Standard Time.

Sincerely,

Maria L Brown

Maria L. Brown
Director
University Cashier's Office
North Carolina State University