

141232

November 19, 2018

INSERT ADDRESS LINE 1
INSERT ADDRESS LINE 2
INSERT ADDRESS LINE 3

Dear INSERT PERSON NAME,

ETSU takes privacy and security very seriously, and it is important to us that you are made fully aware of a potential privacy concern. On October 17, 2018 ETSU ITS discovered that an ETSU employee clicked on a phishing email that resulted in an unauthorized person having access to her email mailbox. Immediately upon discovery, ETSU ITS disabled the employee's email access, reset the employee's username and password, and commenced an investigation. During the initial investigation, on October 26, 2018, ITS discovered a second employee email mailbox was also affected as a result of the same phishing email. Immediately upon discovery, ETSU ITS disabled the second employee's email access, reset the employee's username and password, and commenced an investigation.

We do not know for certain that your personal information was actually accessed. We do know that there was a time period between September 25th, 2018 and the discovery dates mentioned above, where an unauthorized person could have accessed the employees' email mailboxes.

We are notifying you, because personal information about you and/or other individuals in your family, household or otherwise, was contained in one of the employee's email mailbox. The types of information present in the email mailboxes include the full name and social security number of each individual listed below. Other information that may have been included is noted next to the individual's name.

INSERT EMPLOYEE NAME, INSERT TYPE OF INFORMATION
INSERT DEPENDENT/BENEFICIARY NAME, INSERT TYPE OF INFORMATION
ETC.

*If individuals other than yourself are listed above, please notify these individuals, direct them to the resources we have established, and provide them with the instructions regarding activating credit monitoring at no cost to them.

ETSU has taken the following steps to protect your personal information:

- Changed the employees' account passwords
- Implemented additional security safeguards related to the employees' ability to access email
- Counseled the employees
- Reported the incident to law enforcement and other appropriate agencies

We do not know that any personal information was actually accessed, just that the potential for access existed. Out of an abundance of caution we wanted to inform you of the current situation and offer you credit monitoring for one year at no cost to you. Instructions on activating the credit monitoring service are attached. Additionally, you are strongly encouraged to consider taking the following steps to minimize the risk to personal information:

- Request and review credit report
- Contact the national credit bureaus to request a fraud alert
- Contact the national credit bureaus to request a credit or security freeze
- Change credit and banking passwords
- Be vigilant in monitoring credit and banking transactions

We would like to assure you that no other ETSU systems were affected. ETSU is committed to protecting your personal information. ETSU implements state of the art cybersecurity technologies, such as next-generation firewalls, email security, anti-spam, anti-phishing, and anti-malware tools to protect its network and systems.

Information regarding AllClear services, as well as additional information to assist individuals was included in the notice sent and on the website referenced above.

ETSU has taken the following steps to protect personal information following this event:

- Changed the employees' account passwords
- Implemented additional security safeguards related to the employees' ability to access email (2 factor authentication)
- Counseled the employees
- Notified consumer reporting agencies (e.g. Equifax, Transunion and Experian)
- Reported the incident to law enforcement and other appropriate agencies

In addition to the above actions, ETSU is currently investigating additional training opportunities and evaluating workflows and processes that involve the electronic transmission of personal information.

If you require further information concerning the above event, please do not hesitate to reach out to me.

Most sincerely,



Lindsay A. Daniel, Esq.

Enclosures:
ETSU Sample Notice

Cc:
Office of Consumer Affairs and Business Regulation
501 Boylston St.
Suite 5100
Boston, MA 02116

We are grateful for the work that each of you do. We appreciate your support and understanding as we work together to continuously improve our institutional cybersecurity. Please do not hesitate to contact us with questions or concerns. **Please visit the following website for more information: <https://www.etsu.edu/privacy> or contact us via telephone: 423-439-3338 Monday through Friday between 8am and 4:30pm.**

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-434-8081 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by calling 1-855-434-8081 using the following redemption code(s):

INSERT EMPLOYEE NAME, REDEMPTION CODE
INSERT DEPENDENT/BENEFICIARY NAME, REDEMPTION CODE

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate your monitoring options



Lori Erickson

Executive Director
ETSU Office of Human Resources

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.