



Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street, 20th Floor
Philadelphia, PA 19103-3222
T: 215.299.2000 F: 215.299.2150
www.foxrothschild.com

RECEIVED

FEB 16 2018

CONSUMER PROTECTION

Kevin P. Dermody
Direct Dial: (215) 444-7159
Internet Address: kdermody@foxrothschild.com

February 14, 2018

Via Federal Express Only
Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Thomas Edison State University – Notice of Data Breach

Dear Attorney General MacDonald,

In accordance with N.H. Rev. Stat. § 359-C:20, I am writing to inform you of a data security incident that pertains to residents of the State of New Hampshire.

On January 26, 2018, Thomas Edison State University (“Thomas Edison”), a New Jersey State institution of higher education located at 111 W. State Street, Trenton, New Jersey 08608, discovered that an unauthorized user accessed a Thomas Edison employee’s email account (the “Unauthorized User”). Based upon its investigation to date, Thomas Edison reasonably believes that the Unauthorized User improperly acquired the personal information of 557 individuals, including 2 residents of New Hampshire. The personal information acquired includes names and Social Security numbers. This incident was isolated to a single email account and the Unauthorized User did not gain access to Thomas Edison’s network.

Concurrently with sending this letter, Thomas Edison is sending letters to the residents of all impacted states, including New Hampshire residents. For your information, I have enclosed a sample copy of that letter. Notification was not delayed due to a request from law enforcement.

Thomas Edison has moved swiftly to address this unfortunate incident. As soon as Thomas Edison learned of the incident, it removed the impacted email account and computer from its network and contacted experts in the data security and the data breach response fields for guidance. Thomas Edison is in the process of completing a total audit and overhaul of its security infrastructure by information security and technology experts to ensure that an incident like this never happens again. This includes investigating adding further restrictions on accessing Thomas Edison computers and adding additional layers of protection to the Thomas Edison network.

A Pennsylvania Limited Liability Partnership

ACTIVE\53556590.v1-2/14/18

California Colorado Connecticut Delaware District of Columbia Florida Illinois
Minnesota Nevada New Jersey New York Pennsylvania Texas Washington

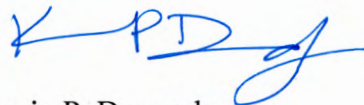
Attorney General Gordon MacDonald
Office of the Attorney General
New Hampshire
February 14, 2018
Page 2

To date, Thomas Edison has not uncovered any evidence that any email account other than the single, impacted email account was accessed or affected by the Unauthorized User. Additionally, Thomas Edison has not seen any evidence that the information obtained by the Unauthorized User has been used or further disclosed. Thomas Edison has filed a police report in this matter with the New Jersey State Police.

As an added precaution, Thomas Edison has offered to the affected individuals, at no cost to them, online credit monitoring and identity restoration services for two years provided by Experian. The enclosed sample notification letter includes instructions on how to use the Experian services.

If you have any questions or would like to discuss this matter further, please do not hesitate to contact me at the address, email or telephone number located at the top of the first page of this letter. Thank you.

Very truly yours,



Kevin P. Dermody

KPD/kpd
Enclosures

cc: Thomas Edison State University



167 W. Hanover St.
Trenton, NJ 08618
www.tesu.edu

Office of the Registrar
(609) 984-1180
Fax: (609) 292-1657

Logo/Client Name
February 12, 2018

[Name]
[Address]
[City State Zip]

RE: Notice of Data Breach

Dear [First Name, Last Name]:

Thomas Edison State University ("Thomas Edison") recently detected an event that may affect the security of your personal information. We write to provide you with information about the incident, what actions Thomas Edison took in response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? On Friday, January 26, 2018, we detected suspicious activity within our network and initiated an internal investigation. We retained a leading cybersecurity law firm to assist us. We determined through our investigation that an intruder gained access to the email account of one Thomas Edison employee. Personal information for certain individuals was present in the impacted email account. To date, we have no evidence of any actual or attempted misuse of personal information present in the email account accessed by the intruder.

What Information Was Involved? The information related to you that was contained in the impacted email account during the period in question included your name and Social Security number.

What We Are Doing. We take this incident and the security of your personal information seriously. As part of our ongoing commitment to the security of personal information in our care, we continue to review our existing safeguards, policies, and procedures, and to implement additional protections to secure further the data in our systems. We reported this incident to the New Jersey State Police.

Although we are unaware of any actual or attempted misuse of your information, as an added precaution, we arranged to have Experian protect your identity for 24 months at no cost to you. Please review the instructions contained in the attached *Steps You Can Take to Prevent Identity Theft and Fraud* to enroll and receive these services. The cost of this service will be paid for by Thomas Edison. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains information on what you can do to better protect yourself against the possibility of identity theft and fraud should you feel it is appropriate to do so. You can also enroll to receive the credit

monitoring and identity restoration services we are offering you. It is important to remain vigilant for incidents of fraud and identify theft by reviewing account statements and monitoring your credit.

For More Information. We sincerely regret any inconvenience or concern this may have caused. We understand you may have questions that are not answered in this letter. To ensure your questions are answered in a timely manner, please do not hesitate to contact me by telephone at 1 (609) 777-5680 or toll-free at 1 (888) 442-8372, Monday through Friday from 8:30 a.m. to 4:30 p.m. Eastern Time (excluding U.S. holidays) or email at cpunchello@tesu.edu, or at the address listed on the top of the first page of this letter.

Very truly yours,



Catharine A. Punchello-Cobos
Associate Vice President and University
Registrar

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for 2 years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary 2-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: May 31, 2018 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by May 31, 2018. Be prepared to provide engagement number DB05309 as proof of eligibility for the identity restoration services by Experian.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. You will need to supply your

name, address, date of birth, Social Security number and other personal information. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Contact the Federal Trade Commission, your state Attorney General, or local law enforcement to report suspected identity theft. For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 1 Rhode Island resident may be impacted by this incident. For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. You have the right to file a police report for this incident or if you ever experience identity theft or fraud, and instances of known or suspected identity theft should be reported to law enforcement. Please note that in order to file a police report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. This notice has not been delayed due to a request from law enforcement.