UCONN
UNIVERSITY OF CONNECTICUT

June 14, 2016

Joseph Foster
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301-6397

Via FIRST CLASS MAIL

Dear Attorney General Foster,

In accordance with N.H. Rev. Stat. §§ 359-C:20, please accept this letter as formal notification of a data compromise involving the University of Connecticut. In the spring of 2015, Information Technology (IT) staff in the School of Engineering detected that malicious software, or "malware," had been placed on a number of servers that are part of the School's technical infrastructure over a period of months, with penetration of the servers beginning as early as September 2013. Through a lengthy and complex investigation that is finally nearing completion, it was determined that some of the files maintained on the impacted servers contained personal information, such as names, contact information, Social Security numbers or Individual Tax Identification Numbers (ITIN), employment information, student academic information, research data and School of Engineering admissions data. To date there is no evidence that any data was accessed or disclosed from the School of Engineering's servers; however, there also is insufficient evidence to conclude definitively that data could not have been accessed or disclosed.

Given the inability to definitively provide such assurance, the University has taken appropriate steps to provide notification to potentially impacted individuals and entities. The University provided notification of the incident and partnered early in the investigation process with appropriate law enforcement units and the Privacy Department of the Office of the Attorney General for the State of Connecticut. (The Office of the Attorney General also in part provides legal support and representation to the University of Connecticut as a public constituent unit of higher education of the State of Connecticut.) Notification to potentially impacted consumers has taken place in batches as personally identifiable information was uncovered and last known addresses were verified. A total of 34,382 individuals have been impacted by this data compromise. The last known addresses of 375 of the individuals impacted were identified as being in the State of New Hampshire. For this reason, the University provides you with the required notice under N.H. Rev. Stat. §§ 359-C:20.

Office of Audit, Compliance & Ethics
9 WALTERS AVENUE, BROWN BUILDING, UNIT 5084
STORRS, CT 06269-5084
PHONE 860.486.4526
FAX 860.486.4527
www.audit.uconn.edu

In order to notify the individuals impacted by this incident and help them to protect themselves from potential identity theft, the University has secured the services of ***AllClear ID***. As noted above, as we identified those that were affected by this breach, ***AllClear ID***, on the University's behalf, provided written notification via first class mail to all of the impacted individuals, offering them one (1) year of identity theft protection services at the University's expense. The mailing to the impacted individuals also includes information regarding how to place credit freezes with each of the three major credit bureaus, and other steps the individuals can take to protect themselves. A sample of the notification letter and enclosures provided therewith is enclosed with this letter for your information.

The University of Connecticut takes the protection of personal information seriously and we are taking steps to prevent a similar occurrence. If you require any additional information about the breach and the way it has been handled by the University, we invite you to visit http://securityincident.uconn.edu. The website contains additional details about the incident, provides answers to frequently asked questions for impacted consumers and contains links to press releases UConn issued about the incident and the scope of the systems and data involved in the compromise. Please also do not hesitate to contact me directly at (860) 486-5256 or rachel.krinsky@uconn.edu if I can answer any questions you may have.

Very Truly Yours,

Rachel Rudnick

Rachel Krinsky Rudnick, J.D., CIPP/US
Assistant Director of Compliance/Privacy Officer

Encls.

Office of Audit, Compliance & Ethics
9 WALTERS AVENUE, BROWN BUILDING, UNIT 5084
STORRS, CT 06269-5084
PHONE 860.486.4526
FAX 860.486.4527
www.audit.uconn.edu

UCONN
UNIVERSITY OF CONNECTICUT
9 Walters Avenue • Storrs, CT 06269-5084

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 31, 2016

Dear John Sample,

We are writing to inform you of a data security-related incident that may have involved your personal information. On March 9, 2015, Information Technology (IT) staff in the School of Engineering detected that malicious software, or "malware," had been placed on a number of servers that are part of the School's technical infrastructure over a period of months, with penetration of the servers beginning as early as September 2013.

As part of the complex and thorough investigation that remains underway, it has been determined that some of the files maintained on those impacted servers contained personal information, such as names, contact information, Social Security numbers, employment information, student academic information, research data and School of Engineering graduate level admissions data. To date there is no evidence that any data was accessed or disclosed from the School of Engineering's servers; however, there also is insufficient evidence to conclude that data was not accessed or disclosed. Given the inability to assure that the data has not been accessed or disclosed, the University is taking appropriate steps to provide notification to potentially impacted individuals and entities.

You are receiving this notification because, as part of our ongoing review, your Social Security number (SSN) or Individual Taxpayer Identification Number (ITIN) was recently identified in one or more files stored on School of Engineering servers and/or computers. We want to make you aware of steps you may take to guard against potential identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have AllClear ID protect your identity for twelve (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 twelve (12) months.

> ***AllClear SECURE***: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5757 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
>
> ***AllClear PRO***: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. **You may sign up online at enroll.allclearid.com or by phone by calling 1-855-904-5757 using the following redemption code: Redemption Code.**

Please note: Additional steps may be required by you in order to activate your phone alerts.

01-03-1-00

For more information on this incident and the data involved, we invite you to visit http://securityincident.uconn.edu or call toll-free: 1-855-904-5757.

The University of Connecticut takes the protection of your personal information seriously and is taking steps to prevent a similar occurrence. We sincerely regret any inconvenience or concern caused by this incident.

Very Truly Yours,

Rachel Rudnick

Rachel Krinsky Rudnick, J.D., CIPP/US
Privacy Officer/Asst. Director of Compliance
Office of Audit, Compliance & Ethics
University of Connecticut

Information about Identity Theft Prevention

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 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, 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 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 (7) 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: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes: 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, www.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.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Twelve (12) months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for twelve (12) months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077