OFFICE OF THE GENERAL COUNSEL
Paul J. Angerhofer
University Counsel

July 12, 2017

By Mail

RECEIVED
JUL 17 2017
CONSUMER PROTECTION

Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Notification of Data Incident

Dear Attorney General Foster:

Data security is of utmost importance to Brigham Young University ("BYU") and we regularly review and enhance our information technology ("IT") and cybersecurity systems and processes to protect against cybersecurity incidents. Unfortunately, BYU was recently a victim of a cyberattack that may have put some of our community members' personal information at risk. This notice describes what BYU has learned through our investigation and the steps we have taken in response to the incident.

During a routine cybersecurity review of its IT systems on June 19, 2017, BYU observed unusual activity in connection with a web server that supports certain BYU expense reporting and vendor payment applications. We promptly took steps to investigate and address the situation, including proactively taking the affected web server offline and retaining highly-experienced IT security and forensic experts to assist us. We also notified the Federal Bureau of Investigation about the incident. We thoroughly reviewed and confirmed the security of the affected web server and associated financial applications before restoring the server and applications to service. We will continue to take appropriate steps to minimize the risk of future cybersecurity incidents.

In the course of our investigation, we discovered that a number of scanned documents, which were submitted to BYU in connection with expense reporting and vendor payment activities and stored on the affected web server, were accessed from and downloaded to non-BYU-affiliated IP addresses during a time period between early June to June 19, 2017.

While some of these PDFs likely were legitimately accessed and downloaded by authorized users using a non-BYU device or IP address, BYU has reason to believe that at least some of the documents may have been accessed and downloaded by unauthorized actors. The investigation to date has determined that the vast majority of the documents that may have been accessed by the unauthorized actors did not contain sensitive information. Unfortunately, however, BYU identified a small subset of documents that contained personal information—such as name and Social Security Number.

BRIGHAM YOUNG UNIVERSITY · A-366 ASB · PROVO, UTAH 84602-1333
(801) 422-6727 / FAX: (801) 422-0265 · EMAIL:paul_angerhofer@byu.edu · WEBSITE: ogc.byu.edu

Pursuant to N.H. Rev. Stat. § 359-C:20(1)(b), BYU is notifying potentially affected individuals, including the one New Hampshire resident that may have been affected by the incident. In addition to providing affected individuals with information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, BYU is also providing all affected individuals with twelve (12) months of identity protection services through AllClear ID.

A copy of the notice to be sent by mail to potentially affected individuals on July 12, 2017 is enclosed.

If you have any questions about this incident, please do not hesitate to contact me.

Sincerely,

Paul Angerhofer
University Counsel
Brigham Young University
(801) 422-6727
paul_angerhofer@byu.edu

Enclosure

[BYU official letterhead for Brian K. Evans]

July 12, 2017

[Name of Individual]
[Address]

Re: Notice of Data Breach

Dear [Name],

We recently learned about a security incident potentially affecting personal information relating to you. This notice describes what we know so far, steps we have taken in response to the incident, and actions you may wish to take to protect yourself.

What Happened

During a routine cybersecurity review of its information technology ("IT") systems on June 19, 2017, Brigham Young University ("BYU") observed unusual activity in connection with a web server that supports certain BYU expense reporting and financial applications. We promptly took steps to investigate and address the situation, including proactively taking the affected web server offline and retaining highly-experienced IT security and forensic experts to assist us. We also notified law enforcement about the incident.

During the course of our investigation, we discovered that a number of scanned documents, which were submitted to BYU in connection with expense reporting and vendor payment activities and stored on the affected web server, were accessed from and downloaded to non-BYU-affiliated IP addresses during a time period from early June to June 19, 2017.

While some of these documents likely were legitimately accessed and downloaded by authorized users using a non-BYU device or IP address, we have reason to believe that at least some of the documents may have been accessed and downloaded by unauthorized actors. Our investigation to date has determined that the vast majority of the documents that may have been accessed by the unauthorized actors did not contain sensitive information. Unfortunately, however, we identified a small subset of documents that contained personal information that can be linked to specific individuals.

What Information Was Involved

We believe that personal information relating to you, including your [data elements], may have been included in the documents that may have been accessed and acquired by the unauthorized actors. As noted above, while some of the access and downloads observed during the period of unusual activity may have in fact been legitimate, we are notifying you now of this security incident out of an abundance of caution.

What We Are Doing

We know that privacy and security are important to the BYU community. We regularly review and enhance the BYU IT and cybersecurity systems and processes. In addition to investigating the incident with outside IT security and forensics experts, we have reported the incident to and are cooperating

with U.S. law enforcement. We thoroughly reviewed and confirmed the security of the affected web server and associated financial applications before restoring the server and applications to service. We are also taking steps to notify each individual whose personal information was potentially affected by this incident. We will continue to take appropriate steps to minimize the risk of future cybersecurity incidents.

What You Can Do

To help protect you, BYU has engaged AllClear ID, Inc. to provide you with identity protection services 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 Identity Repair***: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
>
> ***AllClear Credit Monitoring***: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this 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 [1-877-676-0379], using the following redemption code: {RedemptionCode}.
>
> ***Please note***: Additional steps may be required by you in order to activate phone alerts and monitoring options.

As a general rule, we recommend that you remain vigilant about your personal information by regularly reviewing your financial account statements and periodically checking your credit report. Every individual, whether or not their data has been involved in a security breach, can receive one free credit report every twelve months from each of the three nationwide credit reporting agencies:

Equifax	**Experian**	**TransUnion**
800.525.6285	888.397.3742	800.680.7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834
		www.transunion.com

Review the reports carefully for inquiries from companies you did not contact, accounts you did not open, and debts that you cannot explain. Verify the accuracy of your complete name, Social Security number, address(es), and employer(s). Notify the three consumer reporting agencies about any inaccuracies and promptly report any suspicious activity or suspected identity theft to proper law enforcement authorities, including local law enforcement, your state's attorney general, or the Federal Trade Commission ("FTC"). If you make a report to law enforcement, make sure to request a copy of the police report, as you may need to provide copies to creditors to clear up your records. In addition, you may request that the Internal Revenue Service (IRS) mark your account to identify any questionable activity by submitting Form 14039, "Identity Theft Affidavit," for actual or potential identity theft victims. This form is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

You may wish to add a fraud alert to your credit report file to make it more difficult for someone to get credit in your name. A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies at the contact information provided above. The first agency that processes your fraud alert will notify the others to do so as well. Please be aware that a fraud alert may delay your ability to obtain credit.

You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. To place a security freeze (also known as a "credit freeze"), contact the three credit reporting agencies at the contact information provided above. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency.* Please be aware that using a security freeze may interfere with or delay your ability to obtain credit. You may also incur fees to place, lift, and/or remove a security freeze, which generally range from $5-20 per action.

Be vigilant against phishing attacks. Some criminals may use your personal information to contact you posing as a reputable source to try and trick you into providing confidential information (commonly called "phishing"). For example, they might call you or email you pretending to be a trusted party and ask you to confirm sensitive personal information, such as your social security number or financial account information. Please know that we will never ask you to confirm any sensitive personal information by email or over an unsolicited phone call. If you do happen to be contacted with such a request, it is not from BYU, and you should not provide any personal information. For more information on phishing and on how to avoid being a victim of phishing, please see https://www.us-cert.gov/ncas/tips/ST04-014.

For more information about fraud alerts, security freezes, and avoiding identity theft, you can contact any of the three credit reporting agencies (contact information above), your state's regulatory authority, or the FTC (contact information below).

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.IDTHEFT (438.4338)
www.ftc.gov/idtheft

We truly regret any inconvenience this incident causes you. If you have any questions, please call **(855) 398-6442**.

Sincerely,

Brian K. Evans

Chief Financial Officer and Administrative Vice President

AllClear Identity Repair 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 Identity Repair 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 Identity Repair 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 (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair 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, 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 Identity Repair 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 Identity Repair 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; and
- 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 Identity Repair 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, or
  - 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; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair 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 Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- 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 AllClear Identity Repair 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 Identity Repair, 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