

STATE OF NH
DEPT OF JUSTICE

2017 FEB 22 AM 9:18

BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

February 21, 2017

VIA OVERNIGHT MAIL

Joseph Foster
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

Bentley University understands the importance of protecting personal information and is committed to maintaining the privacy and security of its current and former employees' personal information.

On January 23, 2017, Bentley learned that direct deposit account changes had been made for certain employees. Bentley immediately began an investigation to determine the scope of the incident and retained a third party forensics investigator. Through its investigation, it learned that a targeted phishing email message had been sent to certain Bentley University employees. The attacker was able to use the login credentials that the employee provided via the phishing email to access and or view certain information in the employee's Workday account. This information included the bank account number and bank routing information. For some employees, the information included Social Security number.

Bentley provided written notification via U.S. Mail on February 21, 2017, to three (3) New Hampshire residents in accordance with N.H. Rev. Stat. § 359-C:20 in substantially the same form as the letter attached hereto.¹ Notice is being provided in the most expedient time possible and without unreasonable delay. Bentley is also providing affected individuals with two years of credit monitoring and identity theft protection through Experian.

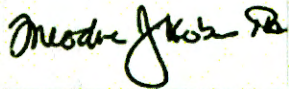
¹ This report is not, and does not constitute, a waiver of personal jurisdiction.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Joseph Foster
February 21, 2017
Page 2

To help prevent something like this from happening again, Bentley is taking steps to enhance its process regarding direct deposit changes and it continues to reeducate its employees regarding phishing emails.

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore J. Kobus III". The signature is written in a cursive style and is contained within a rectangular box.

Theodore J. Kobus III
Partner

Enclosure

[Bentley Logo]

February XX, 2017

[First Name] [Last Name]
[Street Address]
[City], [State] [Zip]

STATE OF NH
DEPT OF JUSTICE
2017 FEB 22 AM 9:18

Dear [First Name] [Last Name]:

Bentley University is committed to maintaining the privacy and security of our employees' personal information. We recently contacted you regarding a phishing incident that affected direct deposit information for some employees. This notification provides additional information about the incident, including steps you can take to protect yourself.

On January 23, 2017, we learned that direct deposit account changes had been made for certain employees. We immediately began an investigation to determine the scope of the incident and retained a third party forensics investigator. Through our investigation, we learned that a targeted phishing email message had been sent to certain Bentley University employees. The attacker was able to use the login credentials that you provided via the phishing email to access and or view certain information in your Workday account. This information included your bank account number, bank routing information and Social Security number.

We recognize this issue can be frustrating and we are taking steps to help protect you and to safeguard the personal information we receive and maintain going forward. We recommend that you remain vigilant toward these phishing scams and to the possibility of fraud and identity theft by reviewing your account statements for any unauthorized activity. You should also contact your bank regarding any unauthorized transactions related to your checking or savings accounts. **We are additionally offering a complimentary two-year membership of Experian's® ProtectMyID® Alert.** This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. ProtectMyID Alert is being paid for by Bentley University and is, therefore, free to you. Enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on ProtectMyID Alert and instructions on how to activate your complimentary two-year membership, please see the next page of this letter.**

We regret any concern this may cause you. To help prevent something like this from happening again, we are taking steps to enhance our process regarding direct deposit changes and we continue to reeducate our employees regarding phishing emails. Should you have further questions regarding this incident and how to avoid phishing scams in the future, please contact Bob Wittstein at ext. 2005 or refer to <http://www.bentley.edu/offices/click-wisely>. If you have questions regarding your personal information or your direct deposit elections, please call me at ext. 2640.

Sincerely,

Ann Dexter
AVP Human Resources

ACTIVATE PROTECTMYID NOW IN THREE EASY STEPS

1. ENSURE **That You Enroll By: May 26, 2017** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: <http://www.protectmyid.com/redeem>**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877.288.8057 and provide engagement #: **PC106600**

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at www.protectmyid.com/redeem
or call 877.288.8057 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877.288.8057.

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll

*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
(800) 685-1111

Experian

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

TransUnion

P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.