BakerHostetler

Baker&Hostetler LLP

999 Third Avenue
Suite 3600
Seattle, WA 98104-4040

T 206.332.1380
F 206.624.7317
www.bakerlaw.com

Randal L. Gainer
direct dial: 206.332.1381
rgainer@bakerlaw.com

March 6, 2017

VIA OVERNIGHT MAIL

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

Re: Incident Notification

Dear Attorney General Foster:

Our client, the University of Idaho, submits this notice after learning of a security incident that may have involved personal information for a New Hampshire resident. On January 24, 2017, the University of Idaho detected that one of its accounts was being used to send phishing email. The phishing email asked the employee to use their email account user name and password to sign-on to a website that appeared to be an Office 365 portal. As a result of this phishing incident, an unauthorized individual may have gained access to the employee's email account, including the messages stored in the account. Upon learning this, the University of Idaho began an investigation and hired a leading computer security firm to assist.

The investigation determined that the employee's email messages contained some personal information of students, employees, and vendors, including names, addresses, and Social Security numbers, and in some cases checking account numbers. Even though the University of Idaho has no evidence that any information has been misused in any way, the University of Idaho is notifying affected individuals and offering them one year of complimentary credit monitoring through Experian.

The University of Idaho provided written notification via U.S. Mail on March 6, 2017, to 1 New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the letter attached hereto.[1] Notice is being provided as expeditiously as

[1] This report is not, and does not constitute, a waiver of the University of Idaho's objection that the State of New Hampshire lacks personal jurisdiction over the University regarding any claims related to the data security incident.

practicable and without unreasonable delay. The University of Idaho has provided contact information so that potentially affected individuals can ask any questions.

The employee's password was changed to prevent any further access to the email account. The University of Idaho is also taking steps to help prevent a similar incident from happening in the future, including evaluating business practices and reeducating its employees regarding phishing emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Randal L. Gainer
Partner

Enclosure

University of Idaho

March 6, 2017

[redacted]

Dear [redacted]: **CSID PIN code:** [redacted]

The University of Idaho is committed to protecting the confidentiality and security of the individual personal information it holds. Regrettably, this notice concerns an incident involving some of that information.

On January 24, 2017, we detected that one of our accounts was being used to send phishing email. The email asked the employee to use their email account user name and password to sign-on to a website that appeared to be an Office 365 portal. The university immediately began an investigation and discovered that an unauthorized individual may have gained access to the employee's email, including the messages stored in the account. Upon learning about the incident, the employee's passwords were changed to prevent any further unauthorized access to their email account, and we expanded the investigation, retaining a leading computer security firm to assist us.

Our investigation determined that the employee's email messages contained personal information for 257 individuals, including yourself. Your personal information included your name, address, and Social Security number. Even though we have no evidence that any of your information has been misused, we are notifying you so that you can take appropriate steps to protect yourself.

To help you protect yourself, the University has worked with CSID to provide one year of CSID Protector services, including credit monitoring and identity theft restoration coverage at no cost to you. In order to activate your CSID Protector coverage, visit https://en.csidprotector.com/enrollment/20?RTN=90000065 to complete a **secure** sign up process and answer some questions to confirm your identity. This process begins by submitting the PIN code at the top of this letter that was provided to you. This PIN code can only be used once and cannot be transferred to another individual.

We advise you to contact any of the major credit reporting agencies to place a fraud alert on your credit report, and to learn about identity theft programs offered by the Federal Trade Commission (FTC). On the following page you will find details on how to contact the credit reporting agencies and FTC.

We are taking steps to help prevent a similar incident from happening in the future, including evaluating business practices and re-educating our employees regarding phishing emails.

We sincerely regret any inconvenience this may cause you. If you have any questions, please call 1-877-274-5565, 24/7.

Sincerely,

Dan Ewart
Vice President for Infrastructure and Chief Information Officer

CSID Protector

After you complete registration for CSID Protector coverage that University of Idaho is providing for you at no charge, you will have increased visibility into possible fraudulent activity so you can respond more quickly if such activity is detected. You will also have team of Identity Restoration Specialists to guide you through the recovery process should you become a victim of identity theft, and you may eligible for reimbursement of certain expenses of up to $1,000,000 subject to the terms and conditions of the applicable insurance policy. University of Idaho encourages you to complete registration as quickly as possible before June 1, 2017, to take advantage of CSID Protector coverage.

The sign-up process is conducted online via CSID's secure website

https://en.csidprotector.com/enrollment/20?RTN=90000065

You will need your CSID PIN Code shown at the top of the first page of this letter. This PIN Code can only be used once and cannot be transferred to another individual. Once you have provided your PIN Code, you will be prompted to answer a few security questions to authenticate your identity, including: previous addresses, names of creditors and payment amounts.

Should you have any questions regarding the coverage or the sign-up process, please contact CSID Member Services at 1-877-274-5565 24/7 or email support@csid.com. Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits

CSID Protector includes:

- **Credit Monitoring**: Monitor your credit file for credit inquiries, delinquencies, judgments and liens, bankruptcies, new loans and more
- **CyberAgent® :** CSID's exclusive Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information online
- **Court Records**: Know if and when your name, date of birth and Social Security number appears in court records for an offense that you did not commit
- **Non-Credit Loans**: See if your personal information becomes linked to short-term, high-interest payday loans that do not require credit inquiries
- **Change of Address**: Find out if someone has redirected your mail to get access to your bank statements, credit card statements and other important identity-related information
- **Sex Offender Monitoring**: Understand if and when any sex offenders reside or move into your zip code, and ensure that your identity isn't being used fraudulently in the sex offender registry
- **Social Security Number Trace:** Know if your Social Security number becomes associated with another individual's name or address
- **Identity Theft Insurance**: You are insured against expenses in the event that your identity is compromised with a $1,000,000 insurance policy
- **Identity Restoration**: Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life

Fraud Alerts

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 6790
Atlanta GA 30374	Allen, TX 75013	Fullerton, CA 92834
1-877-478-7625	1-888-397-3742	1-800-680-7289
www.fraudalerts.equifax.com	www.experian.com	www.transunion.com

In addition to completing CSID Protector enrollment, University of Idaho strongly suggests that you contact the fraud departments of any one of the three major credit-reporting agencies and let them know you may be a potential victim of identity theft. The agency you choose to notify will contact the other two on your behalf. Through that process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission.

We also encourage you to carefully review your credit report(s). Look for accounts you did not open and inquiries from creditors that you did not initiate. Also review your personal information for accuracy, such as home address and Social Security number. If you see anything you do not understand or that is inaccurate, call the credit-reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports or bank account, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need copies of the police report to clear your personal records.

Learn about the FTC's identity theft programs at http://www.ftc.gov/bcp/edu/microsites/idtheft or contact the Federal Trade Commission's toll-free Identity Theft helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261