

Baker Hostetler

Baker & Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

March 15, 2012

Theodore J. Kobus III
direct dial: 212-271-1504
tkobus@bakerlaw.com

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Attorney General Michael A. Delaney

Re: Incident Notification

Dear Attorney General Delaney:

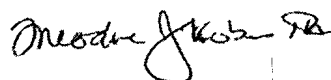
On February 17, 2012, our client, Washington University in St. Louis, discovered that a University employee was copying electronic files onto an external hard drive. While the employee was authorized to see the data in these files, he was not authorized to copy files onto an external hard drive that he brought into the office. The School of Medicine Protective Services responded, and the employee was turned over to police. The hard drive was taken from the employee and is in the University's possession. The employee has been terminated, and the University has referred the matter to law enforcement.

After learning about this incident, the University immediately began a thorough investigation, including hiring an outside forensic firm to try to determine what information was contained on the hard drive and what was done with the information. They determined that the files were copied onto the hard drive but do not know if or how the information was used. The University has no indication that the information was shared with anyone else or was used for fraudulent purposes.

However, because the information found on the hard drive included names, Social Security numbers, addresses and dates of birth, the University, in an abundance of caution, is notifying all employees and job applicants whose information was on the hard drive and offering them one year of free credit monitoring through TransUnion. As a result of this incident, the University is reviewing policies and procedures to determine whether there are measures that might prevent this from happening in the future.

There is approximately 1 New Hampshire resident with his/her information on the hard drive. The University is notifying 1 New Hampshire resident. Notification is being sent to the resident in substantially the form attached hereto.

Very truly yours,



Theodore J. Kobus III

Enclosures



Washington University in St. Louis

SCHOOL OF MEDICINE

March 15, 2012



LV2-82465LV2-0123456 T-
SAMPLE A SAMPLE
123 ANY ST
APT ABC
ANYTOWN, US 12345



Dear Sample A Sample:

The privacy and confidentiality of our employees' and job applicants' personal information is a top priority of Washington University in St. Louis. Regrettably, we are writing to you about an incident related to that information.

On February 17, 2012, a University employee was discovered copying electronic files onto an external hard drive. While he was authorized to see the data in these files, he was not authorized to copy files onto an external hard drive that he brought into the office. School of Medicine Protective Services responded, and the employee was turned over to police. The hard drive was taken from the employee and is in our possession. The employee has been terminated, and the University has referred the matter to law enforcement.

After learning about this incident, we immediately began a thorough investigation, including hiring an outside forensic firm to try to determine what information was contained on the hard drive and what was done with the information. We want to alert you that we found your name and Social Security number on the drive. We are sending this notification to the approximately 4,100 affected employees, former employees and job applicants.

We know the files were copied onto the hard drive but do not know if or how the information was used. We have no indication that the information was shared with anyone else or was used for fraudulent purposes. As a precautionary measure, in order to help you detect possible misuse of your information, we have arranged for you to enroll, at no cost to you, in a three-bureau credit monitoring service for one year provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. For more information on this service and instructions on how to activate your free one-year membership, please see the TransUnion information sheet enclosed.

We want to assure you that we are taking this matter very seriously and are reviewing policies and procedures to determine whether there are measures that might prevent this from happening in the future. We encourage you to take advantage of the free credit monitoring services that we have arranged for you. We deeply regret any concern and inconvenience this situation causes. If you have any questions, please call 1-800-242-5181 Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time and enter or say the following six-digit telephone pass code 445812 when prompted.

Sincerely,

Richard J. Stanton
Associate Vice Chancellor and
Associate Dean, Administration and Finance

82465-LV2

TransUnion Enrollment Information

To enroll in this free service, go to the TransUnion Interactive Web site at www.transunionmonitoring.com and in the "Activation Code" space, enter **ABCDEFGHIJKL** and follow the simple steps to receive your services online within minutes.

If you do not have access to the Internet and wish to enroll in a similar paper-based, credit monitoring service, please call the TransUnion fraud response service hotline at **1-800-242-5181**, Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time. Please enter or say the following six-digit telephone pass code 445812 when prompted. You can sign up for the online or offline credit monitoring service anytime between now and June 15, 2012. Due to privacy laws, we cannot register you directly.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraudulent activity, new inquiries, new accounts, new public records, late payments, change of address and more. The service includes up to \$25,000 in identity theft protection with \$0 deductible. (Certain limitations and exclusions apply).

Whether or not you choose to use TransUnion Interactive's credit monitoring service, 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 unauthorized activity. Under federal law, you may obtain a free copy of your credit report once every 12 months from each of the below three major nationwide credit reporting companies by visiting www.annualcreditreport.com, or by calling 1-877-322-8228:

Equifax
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
1-888-397-3742
P.O. Box 2002
Allen, TX 75013
www.experian.com

TransUnion
1-800-888-4213
P.O. Box 1000
Chester, PA 19022
www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your information is being misused, you may contact TransUnion's Fraud Response Services hotline at **1-800-242-5181** Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time, and enter or say the following six-digit telephone pass code 445812 when prompted, for information and assistance in addressing your identify theft issue. You should also immediately contact the police in your jurisdiction and file a police report of identity theft. Obtain a copy of the police report as you may need to provide copies of the report to creditors to clear up your records. You should also contact the attorney general's office in your home state.



Washington University in St. Louis

SCHOOL OF MEDICINE

March 15, 2012

SSLV1-82465LV1-0123456 T-

SAMPLE A SAMPLE

123 ANY ST

APT ABC

ANYTOWN, US 12345



Dear Sample A Sample:

The privacy and confidentiality of our employees' and job applicants' personal information is a top priority of Washington University in St. Louis. Regrettably, we are writing to you about an incident related to that information.

On February 17, 2012, a University employee was discovered copying electronic files onto an external hard drive. While he was authorized to see the data in these files, he was not authorized to copy files onto an external hard drive that he brought into the office. School of Medicine Protective Services responded, and the employee was turned over to police. The hard drive was taken from the employee and is in our possession. The employee has been terminated, and the University has referred the matter to law enforcement.

After learning about this incident, we immediately began a thorough investigation, including hiring an outside forensic firm to try to determine what information was contained on the hard drive and what was done with the information. We want to alert you that we found your name, Social Security number and date of birth on the drive. We are sending this notification to the approximately 4,100 affected employees, former employees and job applicants.

We know the files were copied onto the hard drive but do not know if or how the information was used. We have no indication that the information was shared with anyone else or was used for fraudulent purposes. As a precautionary measure, in order to help you detect possible misuse of your information, we have arranged for you to enroll, at no cost to you, in a three-bureau credit monitoring service for one year provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. For more information on this service and instructions on how to activate your free one-year membership, please see the TransUnion information sheet enclosed.

We want to assure you that we are taking this matter very seriously and are reviewing policies and procedures to determine whether there are measures that might prevent this from happening in the future. We encourage you to take advantage of the free credit monitoring services that we have arranged for you. We deeply regret any concern and inconvenience this situation causes. If you have any questions, please call 1-800-242-5181 Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time and enter or say the following six-digit telephone pass code 445812 when prompted.

Sincerely,

Richard J. Stanton

Associate Vice Chancellor and

Associate Dean, Administration and Finance

82465-LV1

TransUnion Enrollment Information

To enroll in this free service, go to the TransUnion Interactive Web site at www.transunionmonitoring.com and in the "Activation Code" space, enter **ABCDEFGHIJKL** and follow the simple steps to receive your services online within minutes.

If you do not have access to the Internet and wish to enroll in a similar paper-based, credit monitoring service, please call the TransUnion fraud response service hotline at **1-800-242-5181**, Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time. Please enter or say the following six-digit telephone pass code 445812 when prompted. You can sign up for the online or offline credit monitoring service anytime between now and June 15, 2012. Due to privacy laws, we cannot register you directly.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraudulent activity, new inquiries, new accounts, new public records, late payments, change of address and more. The service includes up to \$25,000 in identity theft protection with \$0 deductible. (Certain limitations and exclusions apply).

Whether or not you choose to use TransUnion Interactive's credit monitoring service, 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 unauthorized activity. Under federal law, you may obtain a free copy of your credit report once every 12 months from each of the below three major nationwide credit reporting companies by visiting www.annualcreditreport.com, or by calling 1-877-322-8228:

Equifax
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
1-888-397-3742
P.O. Box 2002
Allen, TX 75013
www.experian.com

TransUnion
1-800-888-4213
P.O. Box 1000
Chester, PA 19022
www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your information is being misused, you may contact TransUnion's Fraud Response Services hotline at **1-800-242-5181** Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time, and enter or say the following six-digit telephone pass code 445812 when prompted, for information and assistance in addressing your identify theft issue. You should also immediately contact the police in your jurisdiction and file a police report of identity theft. Obtain a copy of the police report as you may need to provide copies of the report to creditors to clear up your records. You should also contact the attorney general's office in your home state.