BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

March 10, 2020

**Via Email (SecurityBreach@atg.wa.gov)**

Office of the Attorney General
1125 Washington St. SE
PO BOX 40100
Olympia, WA 98504

***Re: Incident Notification***

Dear Sir or Madam:

We are writing on behalf of our client, Wichita State University ("WSU"), to notify your office of a security incident involving 2,649 Washington residents. WSU is located in Wichita, Kansas.

In December 2019, WSU learned of a security incident involving unauthorized access to a computer server that WSU used to operate various student and employee web portals. WSU immediately secured this server and engaged a leading computer forensic firm to investigate the incident to determine its scope and impact. The investigation determined that an unauthorized person gained access to this computer server between December 3, 2019 and December 5, 2019. WSU performed a comprehensive review of the server and, on January 13, 2020, determined that information stored in a historical database on the server contained the individuals' names, email addresses, dates of birth, and Social Security numbers.

On March 6, 2020, WSU began mailing notice via postal mail to the potentially affected Washington residents in accordance with West's RCWA § 19.255.010.[1] A copy of the notification letter is enclosed. WSU is offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide affected Washington residents with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. WSU also provided

[1] This report is not, and does not constitute, a waiver of WSU's objection that Washington lacks personal jurisdiction over it regarding any claims related to this data security incident.

a telephone number for potentially affected Washington residents to call with any questions they may have about the incident.

To help prevent an incident like this from happening in the future, WSU is taking steps to enhance their existing security protocols and is re-educating its staff for awareness on these types of incidents.

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

Sincerely,

M. Scott Koller

M. Scott Koller
Partner

Attachment

C/O ID Experts
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-833-570-0375
Or Visit:
https://ide.myidcare.com/wsu
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 6, 2020

Dear <<First Name>> <<Last Name>>:

Wichita State University ("WSU") recently learned of a security incident that may have involved some of your information. We write to provide you with information on the incident, the steps WSU is taking in response to this incident, and steps that you may take to better protect your information, should you feel it is appropriate.

In December 2019, WSU learned of a security incident involving unauthorized access to a computer server that WSU used to operate various student and employee web portals. WSU immediately secured this server and engaged a leading computer forensic firm to investigate the incident to determine its scope and impact. The investigation determined that an unauthorized person gained access to this computer server between December 3, 2019 and December 5, 2019.

WSU performed a comprehensive review of the server and, on January 13, 2020, determined that information stored in a historical database on the server contained your name, email address, date of birth, and Social Security number.

Upon learning of this incident, WSU immediately took steps to respond and worked with outside experts to confirm the nature and scope of the incident and identify individuals whose information may have been stored on the affected server. While WSU does not have any evidence of actual or attempted misuse of your personal information as a result of this incident, out of an abundance of caution, WSU is offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. And, to help prevent a similar incident in the future, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We also encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-570-0375 or going to https://ide.myidcare.com/wsu and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is June 5, 2020.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-833-570-0375, which may be reached Monday through Friday, between 8 am and 8 pm Central Time. WSU will not contact you by phone to request any personal information.

We apologize for any inconvenience or concern this may cause.

MyIDCare™

**Recommended Steps to Help Protect Your Information**

**1**. **Website and Enrollment.** Go to https://ide.myidcare.com/wsu and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at 1-833-570-0375 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

**Credit Bureaus**

| Equifax Fraud Reporting | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-866-349-5191 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5069 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

**New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

**North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. This incident involves approximately 90 Rhode Island residents.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.