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

June 8, 2017

**Via Email (SecurityBreach@atg.wa.gov)**
**And First Class Mail**

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

*Re: Incident Notification*

Dear Attorney General Ferguson:

We are writing on behalf of our client, Washington State University, to notify you of a security incident involving Washington residents.

On April 21, 2017, Washington State University learned that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by the university's Social & Economic Sciences Research Center (SESRC). Immediately upon learning of the theft, the university initiated an internal review and notified local law enforcement. On April 26, the university confirmed that the stolen hard drive contained personal information from some survey participants and, as a result, retained a leading computer forensics firm to assist in the investigation. Not all of the information on the hard drive was encrypted. The hard drive contained personal information of some survey participants and individuals in studies done at SESRC. Personal information was provided by Washington State agencies, colleges and school districts, among others. The personal information included names, addresses, and Social Security Numbers for approximately 1.1 million individuals, and for about 666 individuals, health information. The significant majority of these are Washington residents.

On June 9, 2017, Washington State University will begin providing written notification by U.S. Mail to 723,042 Washington residents in accordance with Wash. Rev. Code §19.255.010, and in accordance to HIPAA for those individuals whose health information was included on the hard drive, in substantially the same form as the enclosed letters. Because the investigation is ongoing, additional Washington residents may be notified in substantially the

same form as the enclosed letters. Washington State University is also offering the potentially affected individuals a free one-year membership in credit monitoring and identity theft protection services from Experian. The university has also provided a telephone number for affected individuals to call with any questions they may have. Notice was provided to the individuals as soon as possible and without unreasonable delay.

To help prevent this type of incident from happening again, Washington State University is strengthening its information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for university employees regarding best practices for handling data, and employing best practices for the delivery of IT services.

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

Sincerely,

Randal L. Gainer
Partner

Enclosures

[Washington State University Logo]

June 9, 2017

<first name> <last name>
<street address>
<city>, <state> <zip code>

Dear <first name> <last name>:

Washington State University is committed to protecting the security and confidentiality of your personal information. Regrettably, we are writing to inform you about an incident involving some of your information that may have been accessed without authorization. Washington State University takes this incident very seriously. We want to provide you with information about what happened and help you take steps to protect yourself and your personal information.

On April 21, 2017, Washington State University learned that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by our Social & Economic Sciences Research Center (SESRC). Immediately upon learning of the theft, we initiated an internal review and notified local law enforcement. On April 26, we confirmed that the stolen hard drive contained personal information from some survey participants and, as a result, we retained a leading computer forensics firm to assist in the investigation.

We know that not all of the information on the drive was encrypted and we have determined that the hard drive contained some of your personal information, including your name, address and Social Security Number.

We have no indication that the information on the hard drive has been accessed or misused in any way. However, as a precaution, we are notifying you of this incident and offering you a complimentary one-year membership to Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. For more information on ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the page that follows this letter.

As president of Washington State University, I deeply regret that this incident occurred and am truly sorry for any concern it may cause you. We are committed to making improvements in our procedures and practices to help prevent this type of incident from happening again. Specifically, we will strengthen our information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for university employees regarding best practices for handling data, and employing best practices for the delivery of IT services.

If you have any questions, please call 1-(866) 523-9195, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

Kirk H. Schulz
President

**How to Activate Your ProtectMyID Membership**

1. **ENROLL** by: **[date]** (Your code will not work after this date.)
2. **VISIT** the ProtectMyID website to enroll: **www.protectmyid.com/redeem**
3. **PROVIDE** your Activation Code: **[code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **[number]**

**Additional Details Regarding Your 12-Month ProtectMyID Membership**

A credit card is not required to enroll in ProtectMyID. Once activated, your ProtectMyID membership includes the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax®, and Transunion® credit files for indicators of fraud.
- **Fraud Resolution:** Toll-free access to U.S.-based customer care and Identity Theft Resolution agents who are available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of fraud resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at www.protectmyid.com/redeem**
**or call 877-371-7902 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 877-371-7902.

**Additional Steps You Can Take**

Even if you choose not to take advantage of the complimentary credit monitoring service 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 free at 877-371-7902. Contact information for the three nationwide credit reporting agencies is as follows:

* 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.

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately 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, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

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.

[Washington State University Logo]

June 9, 2017

Parent(s) or Guardian(s) for
<first name> <last name>
<street address>
<city>, <state> <zip code>

To the Parent(s) or Guardian(s) for <first name> <last name>:

Washington State University is committed to protecting the security and confidentiality of personal information entrusted to us. Regrettably, some of your child's information may have been accessed without authorization. Washington State University takes this incident very seriously. We want to provide you with information about what happened and help you take steps to protect your child and your child's personal information.

On April 21, 2017, Washington State University learned that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by our Social & Economic Sciences Research Center (SESRC). Immediately upon learning of the theft, we initiated an internal review and notified local law enforcement. On April 26, we confirmed that the stolen hard drive contained personal information from some survey participants and, as a result, we retained a leading computer forensics firm to assist in the investigation.

We know that not all of the information on the drive was encrypted and we have determined that the hard drive contained some of your child's personal information, including his or her name and Social Security Number.

We have no indication that the information on the hard drive has been accessed or misused in any way. However, as a precaution, we are notifying you of this incident and offering you a complimentary one-year membership to Experian's® Family Secure®. This product helps detect possible misuse of your family's personal information and provides you and your child with identity protection services focused on immediate identification and resolution of identity theft. In addition, Family Secure will tell you if your child has a credit report, a potential sign that his or her identity has been stolen. Family Secure is completely free to you and your family and enrolling in this program will not hurt your credit score. For more information on Family Secure, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the page that follows this letter. Please note that for your child to receive the complimentary Family Secure product, you, as the parent or guardian, must enroll at the web site with your activation code.

As president of Washington State University, I deeply regret that this incident occurred and am truly sorry for any concern it may cause you. We are committed to making improvements in our procedures

and practices to help prevent this type of incident from happening again. Specifically, we will strengthen our information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for university employees regarding best practices for handling data, and employing best practices for the delivery of IT services.

If you have any questions, please call 1-(866) 523-9195, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

Kirk H. Schulz
President

**How to Activate Your Family Secure® Membership**

1. **ENROLL** by: **[date]** (Your code will not work after this date.)
2. **VISIT** the Family Secure website to enroll: **www.familysecure.com/enroll**
3. **PROVIDE** your Activation Code: **[code]**

If you have questions or need an alternative to enrolling online, please call 877-276-0529 and provide engagement #: **[number]**

**Additional Details Regarding Your 12-Month Family Secure Membership**

A credit card is not required to enroll in Family Secure. To receive the complimentary Family Secure product, you as the parent must enroll at the web site with your activation code listed above. This activation code can only be used by the parent or guardian of the minor. Please keep in mind that once activated, the code cannot be re-used for another enrollment. Once activated, your Family Secure membership includes the following features:

Parent or Legal Guardian:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis

Children:

- Monthly monitoring to determine whether enrolled minors in your household have an Experian credit report
- Alerts of key changes to your children's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity 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 contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee[1]

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, 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 877-276-0529.

**Activate your membership today at https://membership.familysecure.com**
**or call 877-276-0529 to register with the activation code above.**

[1] The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

## Additional Steps You Can Take

Even if you choose not to take advantage of the complimentary credit monitoring service 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 free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately 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, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

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.

[Washington State University Logo]

June 9, 2017

<first name> <last name>
<street address>
<city>, <state> <zip code>

Dear <first name> <last name>:

Washington State University is committed to protecting the security and confidentiality of your personal information. Regrettably, we are writing to inform you about an incident involving some of your information that may have been accessed without authorization. Washington State University takes this incident very seriously. We want to provide you with information about what happened and help you take steps to protect yourself and your personal information.

On April 21, 2017, Washington State University learned that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by our Social & Economic Sciences Research Center (SESRC). Immediately upon learning of the theft, we initiated an internal review and notified local law enforcement. On April 26, we confirmed that the stolen hard drive contained personal information from some survey participants and, as a result, we retained a leading computer forensics firm to assist in the investigation.

We know that not all of the information on the drive was encrypted and we have determined that the hard drive contained some of your personal information, including your name, address, Social Security Number, and personal health information.

We have no indication that the information on the hard drive has been accessed or misused in any way. However, as a precaution, we are notifying you of this incident and offering you a complimentary one-year membership to Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. For more information on ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the page that follows this letter.

As president of Washington State University, I deeply regret that this incident occurred and am truly sorry for any concern it may cause you. We are committed to making improvements in our procedures and practices to help prevent this type of incident from happening again. Specifically, we will strengthen our information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for university employees regarding best practices for handling data, and employing best practices for the delivery of IT services.

If you have any questions, please call 1-(866) 523-9195, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

Kirk H. Schulz
President

**How to Activate Your ProtectMyID Membership**

1. **ENROLL** by: **[date]** (Your code will not work after this date.)
2. **VISIT** the ProtectMyID website to enroll: **www.protectmyid.com/redeem**
3. **PROVIDE** your Activation Code: **[code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **[number]**

**Additional Details Regarding Your 12-Month ProtectMyID Membership**

A credit card is not required to enroll in ProtectMyID. Once activated, your ProtectMyID membership includes the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax®, and Transunion® credit files for indicators of fraud.
- **Fraud Resolution:** Toll-free access to U.S.-based customer care and Identity Theft Resolution agents who are available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of fraud resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at www.protectmyid.com/redeem**
**or call 877-371-7902 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 877-371-7902.

**Additional Steps You Can Take**

Even if you choose not to take advantage of the complimentary credit monitoring service 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 free at 877-371-7902. Contact information for the three nationwide credit reporting agencies is as follows:

* 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.

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately 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, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

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.

[Washington State University Logo]

June 9, 2017

<first name> <last name>
<street address>
<city>, <state> <zip code>

Dear <first name> <last name>:

I am writing to make you aware that we recently learned of a security incident involving some of our community members' personal information. We recently became aware that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by our Social & Economic Sciences Research Center (SESRC), and we confirmed that the stolen hard drive contained personal information from some survey participants. You are receiving this letter because **<variable data -organization's name>** provided data that included personal information to SESRC.

We are approaching this situation with the utmost seriousness and are taking proactive steps to address the situation. Immediately upon learning of the theft, we initiated an internal review and notified local law enforcement. Once we confirmed that the stolen hard drive contained personal information from some survey participants, we retained a leading computer forensics firm to assist in the investigation.

Though there is no evidence the personal information has been accessed or misused, today we are notifying potentially impacted individuals to provide additional information on the incident and guidance on how they can protect themselves. We deeply regret that this incident occurred and are truly sorry for any concern it may cause and are offering one free year of credit monitoring and identity theft protection services to those individuals whose personal information may have been accessed.

At WSU, we remain committed to protecting the security and confidentiality of all personal information. Moving forward, we are making improvements in our procedures and practices to help prevent this type of incident from happening again, including strengthening our information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for university employees regarding best practices for handling data, and employing best practices for the delivery of IT services.

For more information, please visit our website [**insert link**]. Should you have any questions, please don't hesitate to contact me at PresidentsOffice@wsu.edu.

Thank you for your continued partnership.

Sincerely,

Kirk H. Schulz
President