NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

May 11, 2016

Via E-Mail
(SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Olympia School District, to inform you of a potential security incident involving personal information that may have affected approximately 2,145 Washington residents. Olympia School District is notifying affected individuals and outlining some steps they may take to help protect themselves.

On April 12, 2016, an unauthorized individual, impersonating an Olympia School District executive, contacted an Olympia School District employee requesting certain information for Olympia School District employees. Before it was determined that the request was fraudulent, the Olympia School District employee provided a file that contained limited information about some of its employees, including first, middle and last name, address, Social Security number, and 2015 compensation information. After learning of this incident, Olympia School District has investigated this incident and has found no evidence that the unauthorized individual was able to gain access to any Olympia School District systems as a result of this incident or that any other employee information was impacted.

Olympia School District takes the privacy of personal information very seriously, and deeply regrets that this incident occurred. Olympia School District took steps to address and contain this incident promptly after it was discovered. In order to avoid incidents like this from occurring in the future, Olympia School District will be instituting additional employee training or all employees who handle sensitive data. In addition, Olympia School District has contacted law enforcement and will continue to cooperate in their investigation of this incident.

Affected individuals are being notified via written letter, which will begin mailing on or about May 5, 2016. A form copy of the notice being sent to the affected Washington residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

Kristopher Kleiner

KCK
Enclosure

Olympia School District
1113 Legion Way SE • Olympia, WA 98501 • http://osd.wednet.edu

Jennifer Priddy, Assistant Superintendent
Finance & Operations
(360) 596-6129 ~ (360) 596-6121 fax
jpriddy@osd.wednet.edu

NOTICE OF DATA BREACH

[ADDRESS] **May 5, 2016**

Dear [NAME],

We recently learned that the Olympia School District was the victim of a data security incident that affects the personal information of some of our current and former employees. We are providing this notice to inform potentially affected employees about the incident and to call your attention to some steps you can take to help protect yourself. We apologize for any frustration or concern this may cause you. We have arranged for affected current and former employees to receive credit monitoring services for two years and ongoing identity restoration services, each at no cost to you. Instructions for enrolling in these services can be found in the "Information about Identity Theft Protection" reference guide included with this letter.

The district has communicated information about the incident several times, using multiple methods. Please read this communication carefully, as it includes new information and information that is time-critical.

What Happened
On April 12, 2016, an unauthorized individual, impersonating an Olympia School District official, contacted an Olympia School District employee to request certain information for other Olympia School District employees. Before it was determined that the request was fraudulent, an electronic file was provided, which contained information about the affected employees.

What Information Was Involved
The file contained employee information including first, middle and last name, address, Social Security number, and 2015 compensation information. Our investigation has found no evidence that this incident affected any of our network systems or that any other employee information was impacted. Only individuals who received a 2015 W-2 form from the Olympia School District were affected by this incident. No dependent or spouse information was released unless the dependent or spouse also worked for the district in 2015; no banking (direct deposit) information was released; birthdate was not released.

What We Are Doing
We take the privacy and protection of your personal information very seriously at the Olympia School District, and deeply regret that this incident occurred. We have taken steps to address this incident, including promptly alerting affected current employees and working to investigate and remediate the situation. The district has arranged for you to receive two years of credit monitoring from Experian. The service provides:

- Free copy of your Experian credit report

- Surveillance Alerts for:
    - Daily 3 Bureau Credit Monitoring: Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
    - Internet Scan: Alerts if your personal information is located on sites where compromised data is found, traded or sold.
    - Change of Address: Alerts of any changes in your mailing address.

- $1 Million Identity Theft (per **person**) Insurance:* Covers certain costs including lost wages, private investigator fees and unauthorized electronic fund transfers that occur as a result of this incident.
- Lost Wallet Protection: If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- Identity Theft Resolution with ProtectMyID ExtendCARE: The service provides toll-free access to U.S.-based customer care and an Identity Theft Resolution agent who is trained to walk you through the process of fraud resolution if you have any issues with identity theft or fraud on your credit accounts. They will investigate each incident and can help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies. ExtendCARE continues even after your ProtectMyID Elite membership has expired.

For more information about these services and instructions on completing the enrollment process, please refer to the steps described in the "Information about Identity Theft Protection" reference guide included here.

Help with Enrolling in the Experian Product

The Olympia School District will provide a series of drop-in times when employees and former employees can come to the district training/computer lab and get technical assistance to sign up for credit monitoring. The open lab help will take place at the Knox Administration Building, 1113 Legion Way S.E., Olympia, Washington, 98501; Room 308. These drop-in times are:

- May 5, 1:00 – 4:00 p.m.
- May 10, 9:30 – 11:30 a.m.
- May 12, 4:00 – 6:00 p.m.
- May 17, 1:00 – 4:00 p.m.
- May 19, 4:00 – 6:00 p.m.
- May 23, 1:00 – 4:00 p.m.
- June 3, 12:00 (noon) – 5:00 p.m.
- June 17, 12:00 (noon) – 5:00 p.m.
- June 20, 7:00 a.m. – 12:00 (noon)
- June 21st, 7:00 a.m. – 12:00 (noon)
- June 24th, 7:00 a.m. – 12:00 (noon)

Please bring your activation code (unique to you) on the enclosed "Information about Identity Theft Protection" reference guide, and we will help sign you up.

Law Enforcement Notifications

In addition, we have alerted various state and federal agencies, including local law enforcement, the Washington State Attorney General's Office, the Federal Trade Commission, and the U.S. Internal Revenue Service, and we will continue to cooperate with their investigation of this incident.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (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. For more information, please visit https://www.protectmyid.com/million-dollar-insurance.

NOTICE OF DATA BREACH

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, immediately call the credit agency. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of the police report that you file. (Later, you may need to give copies of the police report to creditors to clear up your records.) Also, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

Some of the information affected by this incident could be used to file a fraudulent tax return. As an additional precautionary measure, we also recommend that you file a Form 14039 "Identity Theft Affidavit" with the IRS. For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. If you now live in a different state, there may be similar resources and forms to file in other states, so we recommend that you contact your state department of revenue directly for more information. The Washington State Attorney General also offers information regarding identity theft protection, which is available at http://www.atg.wa.gov/recovering-identity-theft-or-fraud.

Inappropriate use of your personal information often requires a birthdate, which was not released as part of this data breach. Therefore, we recommend that you consider removing your birthdate by taking the date off of your social media accounts.

Most critical is that you take advantage of the credit monitoring and identity theft protection products that we have purchased for you. Please see the enclosed "Information about Identity Theft Protection" reference guide for directions on how to sign up.

If you have encountered any problems in enrolling in the identity protection services online or over the phone because you have **little or no credit history**, please contact Tricia Kelley at (360) 596-6126 or tkelley@osd.wednet.edu. We will have an Experian representative contact you directly to assist with the enrollment process.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact Tricia Kelley, Olympia School District Finance Specialist, at (360) 596-6126, weekdays between 8:00 a.m. and 5:00 p.m. Pacific Time, or via email at tkelley@osd.wednet.edu. Again, we regret the inconvenience or concern caused by this incident.

Thank you,

Jennifer Priddy, Assistant Superintendent
Olympia School District Finance and Operations

(this page intentionally left blank)

NOTICE OF DATA BREACH

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary two-year membership of Experian's® ProtectMyID® Elite. 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. To enroll, visit **https://www.protectmyid.com/enroll** by **July 31, 2016** and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **877-441-6943** between the hours of 6:00 AM and 6:00 PM (Pacific Time), Monday through Friday and 8:00 AM and 5:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **PC101026**. If you have encountered any problems in enrolling in the identity protection services online or over the phone because you have **little or no credit history**, please contact Tricia Kelley, Olympia School District Finance Specialist, at (360) 596-6126 or tkelley@osd.wednet.edu. We will have an Experian representative contact you directly to assist with the enrollment process.

Your Opportunity to Enroll END DATE is 07-31-2016

Credit Reports: We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may annually obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you would like a copy of your credit report more frequently, you may purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page (your Experian report will be free during the two-year period of credit monitoring). If you purchased credit reports between April 12, 2016 and May 5, 2016, the district will reimburse you for those purchased reports. Please go to http://osd.wednet.edu/media//identitytheft/osd_data_security_expense_reimbursement.pdf to print a copy of the reimbursement form. To receive reimbursement, you must apply for reimbursement by August 5, 2016.

Law Enforcement: You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. *You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.*

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you

Information about Identity Theft Protection (page ii)

place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

If you placed a credit freeze on your account between April 12, 2016 and May 5, 2016, the district will reimburse you for this expense. If you have placed a credit freeze on your account, and would like to lift the credit freeze, the district will pay for the credit freeze to be lifted by July 31, 2016. Charges incurred to lift credit freezes cannot be reimbursed after the July 31, 2016 time period. Please go to http://osd.wednet.edu/media//identitytheft/osd_data_security_expense_reimbursement.pdf to print a copy of the reimbursement form. To receive reimbursement, you must apply for reimbursement by August 5, 2016.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

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

Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

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

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872