



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

Alexandria N. Murphy  
Office: (267) 930-1345  
Fax: (267) 930-4771  
Email: amurphy@mullen.law

5133 Harding Pike, B-10, #310  
Nashville, TN 37205-2891

January 26, 2021

**VIA E-MAIL**

Office of the Attorney General  
Security Breach Notification  
200 St. Paul Place, 25th Floor  
Baltimore, MD 21202  
E-mail: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Puget Sound Educational Service District (“PSESD”), located at 800 Oakesdale Ave SW, Renton, Washington 98057, and write to notify your office of an incident that may affect the security of certain personal information relating to five (5) Maryland residents. PSESD is a regional educational agency that serves school districts and state approved charter and private schools in Washington. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PSESD does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

PSESD first learned of unusual activity on its computer network on or about July 25, 2020. Since discovering the activity, PSESD took portions its network offline and commenced an investigation into the event that included working with third-party computer forensic specialists to determine the nature and scope of the event. During the course of the investigation, PSESD learned that certain employee email accounts were accessed by unauthorized individual(s) on separate occasions between April 5, 2020 and August 6, 2020. The investigation found no evidence of specific access to the contents of emails within the impacted email accounts, but could not rule it out. Accordingly, as a precaution, PSESD conducted an extensive review of all messages and documents to determine what information was potentially accessible and to whom the information related. PSESD confirmed on December 23, 2020 the population of individuals whose personal information was potentially accessible. The types of personal information relating to Maryland residents included name, address, and health information.

### **Notice to Maryland Residents**

On or about January 26, 2021, PSESD provided written notice of this incident to affected individuals, which includes five (5) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. PSESD also posted notice of this incident on its website on January 11, 2021 and provided notification to statewide media in Washington on January 11, 2021.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, PSESD moved quickly to investigate and respond to the incident, assess the security of PSESD systems, and notify potentially affected individuals. PSESD notified federal law enforcement and continues to evaluate ways to improve its existing protections to secure the information within its network. PSESD is also providing access to credit monitoring services for twelve (12) months, from TransUnion (through Epiq), to individuals whose Social Security number or driver's license was potentially affected by this incident, at no cost to these individuals.

Additionally, PSESD is providing impacted individuals with guidance on how to better protect against identity theft and fraud, by reviewing their account statements, medical bills, explanation of benefits (EOBs), and credit reports for suspicious charges or claims. PSESD is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. PSESD is also notifying other state regulators as necessary.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1345.



Alexandria N. Murphy of  
MULLEN COUGHLIN LLC

ANM/nsj  
Enclosures

# **EXHIBIT A**



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

<<Variable Heading>>

Dear <<Name 1>>:

Puget Sound Educational Services District (“PSESD”) writes to notify you of an incident that may affect the privacy of your personal information. While we have no reports of fraud or misuse of your information, we are providing you with information about the event, the steps we are taking in response, and additional steps you can take, should you feel it is appropriate to do so.

**What Happened?** PSESD first learned of unusual activity on our computer network on or about July 25, 2020. Since discovering the activity, PSESD took portions of our network offline and commenced an investigation into the event that included working with third-party computer forensic specialists to determine the nature and scope of the event. During the course of the investigation, PSESD learned that certain employee email accounts were accessed by unauthorized individual(s) on separate occasions between April 5, 2020 and August 6, 2020. Our investigation found no evidence of specific access to the contents of emails within the impacted email accounts, but could not rule it out. Accordingly, as a precaution, we conducted an extensive review of all messages and documents to determine what information was potentially accessible and to whom the information related. PSESD confirmed on December 23, 2020 that your personal information was potentially accessible.

**What Information Was Involved?** Our investigation determined your name, <<Data Elements>> were potentially accessible. We note that we have received no reports that any personal information was subject to fraud or misuse.

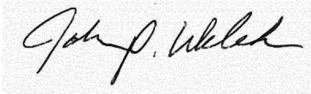
**What We Are Doing.** We take this incident and the security of personal information entrusted in our care very seriously. Upon discovery of the unusual activity, we immediately took portions of our network offline and commenced an investigation that included working with computer forensic specialists to understand the nature and scope of the event. While we have received no reports that any accessible information was subject to actual or attempted misuse, we are providing you with the enclosed *Steps You Can Take to Protect Personal Information*, which includes resources you may take advantage of, should you feel it appropriate to do so. We also continue to evaluate ways to improve our existing protections to secure the information within our network.

**What You Can Do.** PSESD encourages you to remain vigilant against incidents of actual or attempted fraud or misuse from any source and to review the enclosed *Steps You Can Take to Protect Personal Information* for additional action you may take to protect your information.

**For More Information.** If you have questions that are not addressed in this letter, please call our dedicated assistance line at 1-800-223-0837, available Monday through Friday, from 6:00 a.m. to 6:00 p.m., Pacific Time.

We sincerely regret any inconvenience or concern this event may cause you. Protecting personal information is a top priority for PSESD and we remain committed to safeguarding the personal information in our care.

Regards,

A handwritten signature in black ink, appearing to read "John P. Welch", is centered within a light gray rectangular box.

John Welch  
Superintendent  
Puget Sound Educational Services District

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### **Monitor Accounts, Financial and Medical Billing Statements**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, medical bills, explanation of benefits (EOBs), and credit reports for suspicious charges or claims. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**Change Duplicate Passwords.** If the personal information affected for you includes username (or email) and password, PSESD encourages you, if you have not already done so, to change your password to any potentially affected online account and the password to all other online accounts for which you use the same username or e-mail address and same or similar password.

*For District of Columbia residents,* the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>.

*For Maryland residents,* the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8663; and [marylandattorneygeneral.gov](http://marylandattorneygeneral.gov).

*For 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.

*For New York residents,* 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/>.

*For North Carolina residents,* the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island Residents,* the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.