



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>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

RE: Important Security Notification. Please read this entire letter.

Dear Employee:

We are contacting you regarding a recent data security incident. On November 1, 2018, it was discovered that one internal district shared folder containing certain employees' personal information was potentially subject to access by another OJR School District employee. The file contained personal information of 2,734 individuals including certain individuals' names, Social Security numbers and dates of birth. As a result, your personal information may have been potentially exposed to other employees within the OJR School District. Rest assured, the District's data and your personal information was never exposed externally.

What Did We Do to Protect Your Information?

Please be assured that we took immediate action when notified of the incident, and that we are committed to fully protecting all of the information that you have entrusted to us. Owen J. Roberts School District worked with data privacy experts and other professionals to further protect your privacy. We are concerned about our valued workforce and have already taken steps to fix the issue and strengthen our systems, and will continue to do so throughout this response process and beyond. In addition, Owen J Roberts School District has undertaken the following measures to further protect your information:

- Implemented additional security measures and access controls for employees for shared drives;
- Retained outside cybersecurity counsel;
- Safety Protocol and Policies; and
- Flagged affected employee accounts internally.

In addition, and to help protect your identity, we are offering a complimentary one-year membership in TransUnion's *myTrueIdentity* Credit Monitoring Service. 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.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [REDACTED] and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode [REDACTED] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.
- You can sign up for the online or offline credit monitoring service anytime between now and [REDACTED]

Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- 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 credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do to Protect Your Information

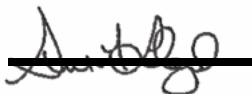
Please remain vigilant by reviewing account statements and monitoring free credit reports. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the enclosed list of additional actions to reduce your chance of identity theft below, including the contact information for the three major credit reporting agencies and the Federal Trade Commission. Individuals can obtain information from these sources regarding fraud alerts and security freezes.

As we go through this process I would ask the following:

1. Please let us know if you learn of or experience any suspicious activity with your credit cards, bank accounts or tax return processing. If you suspect identity fraud, you should report it to a law enforcement agency. We will cooperate with any investigations that state and federal law enforcement open, and provide any information we can to assist their efforts.
2. Report any suspected incidents of identity theft to law enforcement or your Attorney General's Office.
3. Please remain vigilant by reviewing account statements and credit reports.
4. Be aware of your rights under the Fair Credit Reporting Act, including the right to access your credit report, limit access of your credit report to those with a valid need, correct inaccurate information, remove outdated information, protect personal account numbers, and receive notification of possible negative information.
5. Trust that we are doing, and will continue to do, everything possible to protect your personal information and reduce the likelihood of any further problems.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 888-510-9742, Monday through Friday, between 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays.

Sincerely,



Dr. Susan T. Lloyd
Superintendent of School
Owen J. Roberts School District

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➤ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

➤ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies.

➤ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

➤ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.
- Individuals can obtain information about steps to avoid identity theft from any of the above credit reporting agencies or the Attorney General.