

Notice of Possible Unauthorized Disclosure of Student's Name, Address, Birthdate, Social Security Number, Parent/Guardian Name, and Phone Number

Please be informed that Archer City ISD has been informed that your child's personally identifiable information, including his/her name, address, birthdate, social security number, parent/guardian name, and phone number ("Sensitive Data") may have been compromised through a computer security breach. Specifically, Region 9 Education Service Center ("Region 9 ESC") contracted with Archer City ISD to assist it in housing data and transferring student information to the district's electronic cafeteria management system. While providing those services, the Sensitive Data was placed on a file transfer server by Region 9 ESC that it believed to be password protected. Upon its review of the configuration of the temporary server, Region 9 ESC discovered that the Sensitive Data was available for unprotected access. Region 9 ESC cannot unequivocally state that Sensitive Data was not accessed by one or more unauthorized individuals during the period of time the data was on the server unprotected. Immediate steps have been taken to secure the data breach and there is no longer a risk of unauthorized access; however, Region 9 ESC is informing you about this situation so that you may take steps to protect your child against any potential unauthorized access prior to April 21, 2017.

In addition to this general Website notification of a potential breach of your child's Sensitive Data, Region 9 ESC is mailing individual letters to parents of currently enrolled students and to any former students who may have been impacted by the breach. Please watch for these letters this week.

Region 9 ESC strongly recommends that you closely monitor your child's financial circumstances for any suspicious or fraudulent activity. The Federal Trade Commission recommends:

Step 1: For students age 18 and older, place a fraud alert on your credit reports, and review your credit reports. Once you place a fraud alert on your file, you are entitled to order one free copy of your credit report from each of the three consumer reporting companies. You may contact any of the three consumer reporting companies at:

<u>Equifax</u> : 1-800-349-9960	www.equifax.com
<u>Experian</u> : 1-888-EXPERIAN (397-3742)	www.experian.com
<u>TransUnion</u> : 1-888-909-8872	www.transunion.com

For students age 17 and younger, parents may place a fraud alert on their child's credit reports and may request a copy of the child's credit report through *one* of the three major credit reporting agencies. Each credit agency will contact the other two agencies to let them know a Fraud Alert has been placed. (Student and parent information and identifying documentation will be required by the agency in order to provide a report.)

<u>Equifax</u> : 1-800-349-9960	www.equifax.com
<u>Experian</u> : 1-888-EXPERIAN (397-3742)	www.experian.com
<u>TransUnion</u> : 1-888-909-8872	www.transunion.com

Step 2: Immediately close any accounts that you know, or suspect, have been tampered with or opened fraudulently.

Step 3: If you find fraudulent activity on your account, file a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline at 1-877-438-4338, online at <https://www.identitytheft.gov/>, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

Step 4: If fraudulent activity is detected, file a police report with your local police or the police in the community where the identity theft took place.



Please visit the following website for additional important information regarding the steps set forth above:
<https://www.identitytheft.gov/Info-Lost-or-Stolen>.

Region 9 ESC is working with Experian to provide additional identity theft assistance to your child, including consumer fraud protection measures. More information about this additional assistance will be included in your notification letter from Region 9 ESC.

Region 9 ESC deeply regrets any inconvenience this may cause, and thanks you for your understanding and vigilance in this matter. If you have additional questions, please contact the office of Darren Francis, Deputy Executive Director, or Wes Pierce, Executive Director at (940) 322-6928.