Mike Markoe, Ed.D.
Deputy Superintendent

191 South East Street
Frederick, MD 21701

PHONE 301-696-6860
FAX 301-696-6961

Frederick County Public Schools
Reach. Challenge. Prepare.

Laura Nibbs, Senior Executive Secretary
laura.nibbs@fcps.org

Kay Bellucci, Budget Coordinator
kay.bellucci@fcps.org

NOTICE OF DATA BREACH

I am writing to notify you of a data security incident that may have affected your personal information. We take the privacy and security of your information very seriously which is why we are notifying you of this incident, offering you credit and identity monitoring services and informing you about additional steps you can take to protect your personal information.

What Happened? On August 31, 2016, Frederick County Public Schools (FCPS) was informed by a former student that student information may have been accessed without authorization. FCPS conducted a comprehensive internal investigation and concluded that the incident did not occur within the FCPS system. On September 13, 2016, FCPS alerted the Maryland State Department of Education (MSDE) because the same student information was hosted within the MSDE system, indicating that the information may have been obtained from the MSDE system. MSDE investigated the matter until December 2016 and communicated that its system was attacked, but could not conclusively determine when or how this breach occurred. It has since taken steps to increase the security of its system.

What Information Was Involved? The information contained names, Social Security numbers and dates of birth. However, the information did not contain personal financial information (i.e. no credit card nor bank information), phone numbers, street addresses, or other personally identifiable information.

What Are We Doing? FCPS contacted the Federal Bureau of Investigation (FBI) for further investigation. The FBI was unable to identify the data source of access and has since closed its investigation. In accordance with Maryland law, FCPS has contacted the Office of the Attorney General and the Department of Information Technology. In addition, FCPS has increased its own security to prevent a similar incident in the future. For example, FCPS no longer collects students' Social Security numbers and FCPS has removed Social Security numbers from its data system. Also, FCPS is eagerly participating in an Interagency Internal Audit Authority (IIAA) audit and has taken the additional step of hiring an outside cyber security specialist to investigate our data system and provide recommendations. Next, the Board of Education is seeking confirmation from MSDE that its current data system is secure prior to approving any future transmittal of FCPS data to them. Finally, the Board is scheduled to begin discussion at its January 25, 2017 meeting to develop a policy on data breach security and notification processes.

What You Can Do: We encourage you to follow the recommendations on the following page to protect your personal information. You can also enroll in the services we are offering through our trusted partner Kroll, a global leader in risk mitigation and response, to protect your identity for 24 months at no cost to you. The services will include credit monitoring, Web Watcher, and identity consultation and restoration. These services are available to you immediately upon receiving this notice and can be used at any time during the next 24 months. If warranted and requested, an extension of this protection may be considered beyond 24 months. Visit **<<URL will be here>>** to take advantage of these services. Your membership number is **<<PERSONAL ID# will be here>>.** To receive credit services by mail instead of online, please call 1-xxx-xxx.xxxx.

For more information: Further information about how to protect your personal information appears on the following page. If you have questions, please call 1-xxx-xxx-xxxx Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

Sincerely,

Dr. Mike Markoe
Deputy Superintendent

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain aware by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Additional Free Resources: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and www.ftc.gov/idtheft	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
1-877-438-4338	1-888-743-0023	1-877-566-7226	401-274-4400

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.