



April 12, 2011

## **We want to alert you that your personal data may have been stolen**

Our district has been notified by the S.C. Information Sharing & Analysis Center that hackers have captured keystrokes from district computers and figured out district passwords for the State Systems that store the district's student and employee information.

This kind of hacking is not something a person could find just surfing on the internet. It could be done only by skilled computer technicians who were purposely trying to capture this information.

It is our understanding that the hackers then used the passwords to access students and employee data in the State System. While the details of the origin of access and/or cause of this breach are unknown at this time, we immediately shut down the affected computers as a safeguard and notified SLED. We are working in cooperation with law enforcement to take all appropriate investigative actions.

Although we have no way of verifying which information was compromised, the information which **could** have been compromised includes any information in your file in the data base, including your name, social security number, birth date, address, and home and work phone numbers.

To date, there is no evidence that any confidential information has been used illegally. If you would like to take additional measures to protect yourself, you should consider the following information.

- ◆ Be vigilant and carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved and contact the Federal Trade Commission for further guidance.
- ◆ Tips on how to guard against misuse of personal information can be found on the Federal Trade Commission website at [www.ftc.gov](http://www.ftc.gov). This site should help you to determine what to look out for with regard to your personal financial information.
- ◆ You DO NOT have to close your bank account or cancel your credit cards. You may want to review your credit report. By law, you are entitled to one free credit report each year, and this report can alert you to any suspicious activity on your accounts. To request a free credit report from one of the three major credit bureaus – Equifax, Experian, or TransUnion – contact their fraud protection departments at either the phone number or address or go to the website: [www.annualcreditreport.com](http://www.annualcreditreport.com).
- ◆ A fraud alert with the National Credit Bureau is a more proactive measure you can take to protect yourself, if you feel it is necessary. You can request that the three major credit

bureaus place a fraud alert on your credit bureau records. A fraud alert is a message that credit issuers receive when someone applies for new credit in your name. The message tells creditors that there is a possible fraud associated with the social security number and gives them a phone number to call (yours) before issuing new credit.

You can contact the fraud alert departments at any one of the three major credit bureaus:

**TransUnion**

Direct Line for reporting suspected fraud:  
1-800-680-7289  
Fraud Victim Assistance Department  
PO Box 6790  
Fullerton, CA 92634  
Phone 800-916-8800 / 800-680-7289  
<http://www.transunion.com>

**Experian**

Direct Line for reporting suspected fraud:  
1-800-397-3742  
Credit Fraud Center  
PO Box 1017  
Allen, Texas 75013  
888-EXPERIAN (888-397-3742)  
<http://www.experian.com>

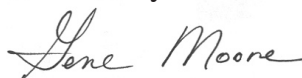
**Equifax**

Direct Line for reporting suspected fraud:  
1-800-525-6285  
Fraud Division  
PO Box 740250  
Atlanta, GA 30374  
800-685-1111 / 888-766-0008  
<http://www.equifax.com>

Again, at this time, we have no indication that this confidential information has been used illegally. Nevertheless, we believe it was necessary to notify you of this security breach and provide you with information regarding possible steps you may wish to take to address it.

We sincerely regret any inconvenience this incident may cause. If you have any questions about this matter, please contact our Computer Security Taskforce at 803-416-8822 or [computersecurity@lcsd.k12.sc.us](mailto:computersecurity@lcsd.k12.sc.us).

Sincerely,



Gene Moore  
Superintendent