

NOTIFICATION OF DATA THEFT

WHAT HAPPENED?

A laptop computer was stolen on February 22, 2007, from the home of an employee of the Ohio Auditor of State's Office. Employees of the Office of the Auditor are responsible for reviewing and evaluating financial information about the district as it relates to the district's routine annual audit, the district's comprehensive annual financial report, the special performance audit, and the audit of the 5 year forecast required by the district's status in fiscal emergency. The stolen laptop included files created in the spring of 2006 that contained employee information including social security numbers. However, access to files on the laptop was password protected. An attorney for the Auditor of State's Office has informed us that a police report has been filed.

WAS MY SOCIAL SECURITY NUMBER IN THE FILE?

You will receive a form letter at your home address advising you of the incident if your identifying information was included in the files on the laptop.

AM I A VICTIM OF IDENTITY THEFT ?

Not necessarily. Identity theft is the unauthorized use of personal identification to commit fraud or other crimes. At this time, the information on the laptop might be considered as an occurrence of data theft. There is no reason to believe that information on the laptop was the intended target of the thieves. Laptops are issued to most audit staff to simplify collection of information during audits. Those laptops require login with user name and password before any files can be viewed. While there is no indication that your information has been misused or disclosed in such a way that would adversely affect you, we want you to be fully informed about this matter.

HOW WOULD I KNOW IF INFORMATION WAS MISUSED?

Routinely monitor your financial accounts and billing statements. Be alert and respond immediately if-

- Bills do not arrive as expected
- Unexpected credit cards or account statements arrive
- Credit is denied for no known reason
- You receive calls or letters about purchases you did not make
- You receive emails, calls or letters asking you for personal information

More detailed information about an appropriate precautionary response can be found at <http://www.ftc.gov/idtheft>. Please consult http://www.antiphishing.org/consumer_recs.html to protect your identity against email scams.

WHAT SHOULD I DO NOW?

To protect against misuse of your personal information, you can place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax
800-525-6285

Experian
888-397-3742

TransUnionCorp
800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, contact the creditor involved. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

WHO CAN I TALK TO ABOUT THIS?

Plan to attend the Data Theft Information Meeting that will be scheduled at South High School on waiver Wednesday, March 28, 2007. Please attend either the morning session between 8:00 and 8:30 a.m. or the afternoon session between 2:30 and 3:30 p.m. in the South High School Commons/Cafeteria. If you have immediate concerns, please call Becky Scovill, Payroll Supervisor, at 505-2817.

ARE THERE ADDITIONAL PRECAUTIONS?

Routinely review your credit report for accuracy. To obtain a free credit report once a year, visit <http://www.annualcreditreport.com> or call 877-322-8228. A credit report includes information on where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy. Nationwide consumer reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home.

You may order your reports from each of the three nationwide consumer reporting companies at the same time, or you can order your report from each of the companies one at a time. The law allows you to order one free copy of your report from each of the nationwide consumer reporting companies every 12 months. Only one website is authorized for the free annual credit report you are entitled to under law – <http://www.annualcreditreport.com>.

Other websites that claim to offer “free credit reports,” “free credit scores,” or “free credit monitoring” are not part of the legally mandated free annual credit report program. In some cases, the “free” product comes with strings attached. For example, some sites sign you up for a supposedly “free” service that converts to one you have to pay for after a trial period. If you don't cancel during the trial period, you may be unwittingly agreeing to let the company start charging fees to your credit card.

Some “imposter” sites use terms like “free report” in their names; others have URLs that purposely misspell <http://www.annualcreditreport.com> in the hope that you will mistype the name of the official site. Some of these “imposter” sites direct you to other sites that try to sell you something or collect your personal information.

www.annualcreditreport.com and the nationwide consumer reporting companies will not send you an email asking for your personal information. If you get an email, see a pop-up ad, or get a phone call from someone claiming to be from <http://www.annualcreditreport.com> or any of the three nationwide consumer reporting companies, do not reply or click on any link in the message. It's probably a scam. Forward any such email to the FTC at <http://www.spam@uce.gov>.

SHOULD I BUY IDENTITY THEFT COVERAGE?

This is your decision. Some products offer you protection against the costs associated with resolving an identity theft case. When deciding whether or not to purchase identity theft insurance, please consider that the law provides significant protection to victims of identity theft. Also some homeowner's or renter's insurance might already provide you with identify theft protection. Some district employees have already enrolled in the identity theft protection plan through Pre-Paid Legal Services.

WHAT WILL THE DISTRICT DO TO PROTECT MY IDENTIFYING INFORMATION?

The district had already begun a process to convert the employee numbers currently in use (group code + 9 digit social security number) to a variation that includes group code + 2 digit date of birth + the last 4 digits of social security number. Those numbers will be converted by the end of March. The Treasurer's Office, working with the Office of Information Management, has researched document imaging software. A product has been purchased in partnership with the state Management Information Site that will improve the security of data written to files. In addition to providing us a paperless solution to our record retention requirements, the database will provide us with software to redact or make unreadable any confidential information, such a social security number, that occur in any files that we share with the auditor's office in the future.

IS THIS FOOLPROOF?

The district is required to distribute information, including your social security number, to several outside agencies including, but not limited to, Anthem Insurance, MetLife Insurance, Social Security Administration, Ohio Department of Taxation, Ohio Bureau of Employment Services, School Employees Retirement System, State Teachers Retirement System, and the City of Springfield Income Tax Division. The district provides the information according to the format required by the authorized agency. Every attempt is made to protect the data including the use of secure web sites, of password protected file transfer protocol, and of delivery services. According to the Federal Trade Commission, "It is almost impossible to be in business today and not collect or hold personally identifying information –names and addresses, Social Security numbers, credit card numbers, or other account numbers – about your customers, employees, business partners, students or patients." The security of that information is important to all of us at Springfield City Schools.