

WHAT HAPPENED?

We were notified that at about four o'clock this morning, the company that publishes our employee benefit booklets, Systematic Automation—located in Fullerton, California—was burglarized. Three monitors and one computer were stolen. The computer contained information on all district employees, including social security numbers. While the information sent to Systematic Automation was encrypted, when they extract the information it is unencrypted and stored in an Access Database. From the contacts we have had with the company, we question the security of the computer that was stolen.

Please read the information below for recommended next steps.

If after reading the information you have any immediate concerns, please contact Louise Baker, Supervisor of Payroll and Benefits, at 576-4192.

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 computer might be considered as an occurrence of data theft. 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.

We recommend that all Modesto City Schools employees place a fraud alert on their credit file as a preventative measure against identity theft in the event that the data is compromised.

To place a fraud alert, which 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; <http://www.fraudalert.equifax.com>
Experian (888) 397-3742
TransUnion Corp (800) 680-7289.

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 e-mails, 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>.

WHAT SHOULD I DO NOW?

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 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. This suspicious activity, if found, may or may not be related to this incident. You should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

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?

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 identify theft. Also some homeowner's or renter's insurance might already provide you with identify theft protection.

WHAT WILL THE DISTRICT DO TO PROTECT MY IDENTIFYING INFORMATION?

The district is required to distribute information, including your social security number, to several outside agencies. 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 district will be re-evaluating the security measures of all outside agencies to which we send employee information.