



FRAUD TIP OF THE WEEK
***My Personal Information Is In a
Stolen Business Computer - What Should I Do?***

By Detective Paul Henninger
October 2, 2006

This weekend, seven computers were stolen from another government agency in Salem. This agency manages a state program affecting about 4,500 high school students in three counties: Yamhill, Polk and Marion. The office was not protected by an alarm system. The stolen computers had security features activated, so any information on the computers should not be viewable to common identity thieves. The agency has an off-site secured server that stores the type of personal information sought by identity thieves. The thieves will not have access to the server using the stolen computers. The agency will be viewing information uploaded from the server to each computer to see if any student data was on any of the computers at the time of the theft. Any affected student will receive a letter in the mail.

Historically, business burglars have targeted items that could be put to personal use, sold or traded for drugs. Because of the profitability of Identity Theft, many of today's burglars are also looking for paper files and data storage devices, such as computers and PDA's. The personal information inside the computer can be a lot more valuable to the thief than the computer itself.

Businesses and government agencies need to have, and enforce, strict security protocols for handling, storing and disposal of personal information regarding their employees and clients. Site security, locks and alarms are just a start. Files with personal information should be locked. All computers should be password-protected. Ideally, the computers should be password-protected and have encrypted software for maximum protection of information.

For further information about computer and storage device security, read my weekly fraud tip entitled "Traveling Safely With Computers or PDA's." *

What do I do if I am notified my personal information was in a stolen business computer?

TIPS:

- **Don't Panic**

□ **Make an Inquiry.**

- **Ask the business or agency what type of personal information was in the stolen computer:**
 - Date of birth - Yes, you can become a victim of Identity Theft if thieves get your name and date of birth.
 - Social Security number - This is much worse. If a thief can access the computer, you are toast. Consider yourself a victim of identity theft if the computer is not properly safeguarded.
- **Computer Safeguards.** Ask if the computer was password-protected. Password protection will prevent most thieves from viewing data on the computer. Ask if the computer was encrypted. Password protection with encryption will protect the data from even a computer savvy thief.
- **Ask if they are going to provide a free credit monitoring service.**
- **As a side note, ask whether the business releases “directory information” to others.** Is your date of birth part of their directory information that they give out to others without your specific permission? If so, request your information be removed from their directory.

□ **Decide a course of action to protect yourself or your child from Identity Theft.**

1. **At a minimum, monitor your credit reports.** Everyone can get a free credit report from each credit bureau once a year. Federal law requires this. Parents of children can also get a free credit report each year on their children. If you want to order free credit reports for yourself or your child contact the three credit bureaus. This can be done online, using the credit bureaus official website at www.annualcreditreport.com. Caution: This is the only FTC-approved website for a free credit report.
2. **Report the incident.** If you are not satisfied with the computer safeguards of the business, or you discover your personal information is being used, report the incident to your local police department, the Federal Trade Commission (FTC) and the three credit bureaus. It is important to place a fraud alert on your credit history.

For a complete explanation of this reporting process, refer to my fraud tip of the week entitled “What Do I Do If My Identity Is Stolen?” *

3. **Consider using a credit monitoring service, for a fee.** These businesses can assist you in repairing your credit and monitoring your credit history for you.

*The mentioned fraud tips, as well as other fraud tips, can be found on the Salem Police Department’s website at www.cityofsalem.net/departments/police.