

ISSUE #23 – 1st Quarter 2008

Beware – Online Resume Fraud

Be Careful Posting Your Job Resume Online

Identity theft has found a new source for mining personal information: online job resumes. This won't come as good news for those seeking employment or who have posted their resume online.

Consider what is usually found on online resumes: name, age, phone number, home address, education, hobbies, and work references. Collectively, this information can be used for purposes other than for which it was lawfully intended for.

Last year, Monster.com, which is the nation's largest Internet job site, became victimized when thieves hacked into the site and stole the personal information of 1.3 million job seekers. "Thieves will work very hard to get resumes because they are fabulous sources for identity theft," said Pam Dixon, who is executive director of the World Privacy Forum.

Identity theft can even result after one answers a job recruitment ad, like say on Craigslist. "The rule of thumb is: wait for the in-person interview before you give up your bona fides. You've got to be really careful with that," said Dixon in an interview with ABC News in San Francisco.

Dixon offers these tips: Don't post online your home address, phone or Social Security number--unless you are applying to the Federal or State government. Instead provide a disposable email or post office box.

If a potential employer asks for your Social Security number as part of a background check, be careful about this request unless you are first sure of the business's legitimacy. This precaution is necessary due to the high number of fake online job offers, especially those for work-at-home offers.

Seek Job Sites That Allow You to Post Privately

Dixon suggests that "if you're going to post a resume online, post your resume 'privately.'" What this means is that you should take advantage of those job sites which offer anonymous posting that allows you to shield your contact information and email address whenever you post a resume. "Masking this information is perhaps the single most important step job seekers who want to post a resume online can take to protect themselves." Job seekers might feel that they will be hurting their chances with potential employers by choosing this option, but



the alternative can be much worse: your private information falling into the wrong hands.

Recourse for Job Seekers

Contact Identity Fraud, Inc. if you discover that you have been the victim of a job scam. Additionally, you may file a consumer complaint with the FTC by calling (1-877-FTC-HELP) or by using the FTC's online filing system, located at <http://www.ftc.gov/>. Click on "File a Complaint Online." If your personal information was used for illegal purposes, you should immediately file a police report. Please see <http://www.worldprivacyforum.org/jobscamtipspayforwarding.html> for additional tips on how to deal with the aftermath of a job scam.

ALERT-- A Growing Epidemic --ALERT

Just how prevalent is identity theft?

A recent report by the Federal Trade Commission says that 8.3 million Americans were victims of identity theft in 2005. These personal data thefts cost businesses and consumers billions of dollars with estimated losses totaling \$56.6 billion. Separately, according to a recent article in the *San Francisco Chronicle*, online identity theft is not unlike being mugged online by "striking 3.7 percent of all adult Americans, and making it roughly twice the incidence of ordinary street crimes."

If you think you are a victim of identity theft, please contact Identity Fraud, Inc. at:

1-866-4ID-FRAUD
(866-443-3728)