Employers Face Liability for Five Kinds of Identity Theft

By Joanne Deschenaux, SHRM's senior legal editor

ATLANTA—The workplace is the site of more than half of all identity thefts, Michael Hall, a certified identity risk management specialist, told attendees at the SHRM Atlanta Human Resource Conference Oct. 6. There are five types of identity theft, and employers can potentially be held liable for any or all of them, he said. Because "many thieves these days don't care about stealing money; they just want your information, which they can use to make money," he stressed that it is crucially important for businesses to take steps to safeguard employees' personal information.

Types of Identity Theft

Financial identity theft. When thinking about identity theft, most people first focus on the theft of personal information being used to obtain credit cards or to raid existing bank or credit card accounts, Hall said. Thieves can deplete your accounts, run up credit card bills in your name and destroy your credit. But there are other types of identity theft as well, Hall told the session attendees.

Driver's license identity theft. A thief can use your information to acquire a driver's license in your name and claim to be you during a traffic stop. This could result in the suspension or revocation of your driving privileges or in criminal charges for offenses such as driving while intoxicated.

Social Security identity theft. A thief might use your Social Security number to gain employment or to report income under your name. An illegal immigrant may use your Social Security number to get a job. Similarly, a convicted criminal may want to use your number to get around an employer's background check. Thieves also may be interested in getting paid, but not paying taxes. "The Internal Revenue Service and the Social Security Administration don't necessarily talk to one another," Hall said, and there have been instances of people finding out that their tax returns have already been filed and that someone else has received their refunds.

Medical identity theft. This is the fastest growing type of identity theft, Hall observed, noting an AARP study that found that stolen health insurance cards are being sold on the black market for $500 to $600 dollars.

In this type of theft, criminals obtain your health insurance information or Social Security number to get health care. Because this means that your medical history could include someone else's information, this type of identity theft can be life threatening, Hall noted. For example, as a result of someone else pretending to be you, it would be possible for your blood type to be listed incorrectly on your medical records.

Character/criminal identity theft. Your personal information might be given to the police instead of the thief's information. This can result in your arrest for crimes that you did not commit.

Most Identity Theft Starts at Work

Because the workplace is the site of so much identity theft, "executives must stop thinking about data protection as solely an IT problem," he advised. Further, the problem lies not with the data, but with the people. There are five main causes of data breaches at work, Hall noted:

- Disgruntled or dishonest staff.
- Untrained or careless employees.
- Lost or stolen laptops.
- Service providers, contractors and visitors.
- Hackers.

The Federal Trade Commission (FTC) has advised that "information security should be a priority for every business in America," Hall said and added that "any business comes under some information protection law."

[MORE]

These laws (and regulations) include:
• At least 44 state laws concerning identification theft and notification of data breaches.
• The Health Insurance Portability and Accountability Act, for health information.
• The FTC Act, which reaches "unfair and deceptive business practices."
• The Gramm-Leach-Bliley Act for financial information.
• The Fair Credit Reporting Act and the Fair and Accurate Credit Transactions (FACT) Act.
• New federal agency rules for FACT Act compliance, which go into effect on Nov. 1, 2008.

Steps To Take
As an employer, you can be subject to criminal liability for data theft as well as civil liability to employees whose personal information has been stolen. In addition, the company may suffer costly damage to its reputation, Hall warned. There are announcements of data breaches almost every day, he noted. So what can you as an employer do to prevent these breaches? Hall suggested some basic steps:

• **Develop a written data protection plan**.
The plan should be designed to protect all data throughout the company.
• **Appoint a security manager**.
This should be an upper level managerial employee, Hall advised.
• **Provide training for employees**.
Employers should implement a training schedule and ask every employee to sign an agreement that he or she will follow the company standards.
• **Before you outsource any company function**, investigate that firm's data security practices.
• **Consider offering identity theft protection as an employee benefit**.
This typically would include restoration services—help to the employee in reclaiming his or her identity.

Some day soon, you may see an ad on television, Hall said, advising all employees whose personal data has been stolen at the workplace to contact a lawyer for information about suing their employers. You want to do everything you can to prevent such a lawsuit from happening, Hall suggested, but also noted that "you can't prevent all identity theft." However, showing that you took all the steps that you reasonably could have taken will go a long way toward defending a legal action based on theft of employees' personal data.

Joanne Deschenaux is SHRM's senior legal editor.

www.shrm.org/hrnews_published/archives/CMS_026842.asp