WORKPLACE IDENTITY THEFT:
CURING THE LATEST HR HEADACHE

Follow these rules to protect employees and lessen your risk of liability for identity theft.

By Douglas Hottle

Identity theft — the improper or fraudulent use of someone's personal information — is rising, and it's presenting a major headache for employers: They're being held liable for such theft in the workplace. Unfortunately for employers, personal information, such as social security and bank account numbers, is precisely what's contained in employee files, a goldmine for identity (ID) thieves.

Employers unwittingly aid ID thieves by mishandling employees' personal information. Consequently, employers face legal repercussions as victims of such crimes seek restitution. For example, a Minnesota employer was recently sued for faxing a list of employees' names and social security numbers to managers within the organization.

> Personal information is precisely what is contained in employee files, a goldmine for ID thieves.

Eliminate These Mistakes

You can protect employees and minimize the risk of theft and liability by eliminating the more frequent mistakes employers make. Here are rules to remember:

- **Don't keep** files in accessible locations.
- **Lock** file cabinets.
- **Don't place** social security numbers on documents such as time cards, paychecks, licenses, membership cards, or purchase receipts.
- **Never leave** original documents or facsimiles in all-access copiers.
- **Don't use** social security numbers as health plan policy reference numbers.

It's the Law

Given the likelihood of liability when employees' records are misused, employers should take steps to protect personal employee

> Employers unwittingly aid ID thieves by mishandling employees' personal information.

Any hard-copy document containing sensitive data should be destroyed by burning or shredding.

information and, indeed, are required to do so under state and federal statutes. In Pennsylvania, for example, recent legislation provides standards for printing and transmitting social security numbers. This law sets out the following prohibitions:

- **Never put** a social security number on any materials that are mailed to an individual, except where required by federal or state law, such as a W-2 form.
- **Be sure not to post** social security numbers.
- **Don't print** a social security number on any card.
- **Never transmit** a social security number over the Internet without the use of encryption technology.
- **Don't require** online users to access your Web site with a social security number (unless you have password protection or other authentication technology).

You should also become familiar with the Fair and Accurate Credit Act (FACTA). This act states that any hard-copy document containing sensitive data should be destroyed by burning or shredding to make sure the documents can't be reconstructed.

A recent FACTA amendment requires employers to take reasonable measures to dispose of an employee's credit report obtained during the hiring process. Under the statute, reasonable measures may include developing policies that require the destruction of all documents and electronic files containing personal information.

Recent legislation provides standards for printing and transmitting social security numbers.

Other Steps to Take

Beyond following state and federal regulations, here are other steps you can take to protect employees' personal information:

- **Create an ID theft-reporting policy**, and tell employees about it frequently.
- **Screen all employees** (including volunteers) who have access to personal data. Consider conducting background checks when you hire new staff.
- **Keep employees' personal data** in locked cabinets. If the files are stored electronically, make certain these files can be accessed only by appropriate personnel. Use an electronic monitoring system that lets employers see who is attempting to access sensitive information.
- **Never use** social security numbers as reference numbers of any kind.
- **Train employees** about ID theft. Provide instruction on how to secure, handle, and destroy appropriate files. Include information on protecting personal items (such as purses and wallets) and private areas (such as lockers).

If an ID thief is lurking in your workplace, your first line of defense is your organization's policies. Periodically review your policies to ensure accordance with state and federal legislation. You may also want to consider seeking legal help to be certain you're following the law.

Strengthening your policies will go a long way toward minimizing the potential for identity theft and limiting your organization's liability if an ID thief strikes. Adopting a comprehensive series of policies and procedures won't prevent all identity theft (ID thieves are a resourceful lot) nor prevent every lawsuit. But having a policy and following the law will bolster your position in any litigation related to identity theft. ■

Your first line of defense is your organization's policies.

Douglas Hottle (dmh@muslaw.com, 412-456-2809), an attorney with Meyer, Unkovic & Scott in Pittsburgh and Lancaster, Pennsylvania, works primarily in the area of employment law.

Nonprofit World • Volume 25, Number 5 September/October 2007
Published by the Society for Nonprofit Organizations
5820 Canton Center Road, Suite 165, Canton, Michigan 48187
734-451-3582 • www.snpo.org