

UPDATE: Identity Theft and I – 9 Maintenance

Waldthausen & Associates, Inc. is a Retained Executive Search firm with the focus on recruiting managers that influence a company's result and earnings. The firm focuses on recruiting professional managers for US subsidiaries with parent companies located in central Europe.

Warding Off Identity Theft

Question: What steps should we take to ensure our employees' personnel data is protected internally with regard to identify theft concerns? Are there any new laws regarding an employer's responsibility to protect such data?

Answer: Though several federal laws, including the "Identity Theft Protection Act," "Personnel Data Privacy and Security Act of 2005," and "Safeguarding Americans from Exporting Identification Data Act," have been introduced in both Houses of the US Congress, none has yet passed. Several of these bills concern the display of Social Security numbers. At present, many states have passed their own legislation regarding protection of Social Security data.

As an employer, once you receive identity and personal information from an employee, you must take steps to restrict accessibility to such information. This information can be found on many forms including an application or application inserts, a credit or criminal background report, accounting or benefits paperwork, and employment-related records or documents completed by employees. Employers can help prevent identity theft and limit their liability by using some preventative measures:

Assess current practices for the security of personnel information and identify any risks.

Develop a written privacy policy describing in detail the protected information and security practices your company has put in place. Your policy should also address what steps to take and what agencies to alert if a security breach occurs.

Train employees responsible for record security.

Do not collect more information than you need

Strictly limit access to both paper and electronic records – lock file drawers and password-protect electronic files. Change passwords frequently.

Protect employees' Social Security numbers – don't use these numbers as identifier or I.D. numbers. Don't put the SSN on documents where it has no relevancy – time cards, I.D. cards, payroll checks, etc.

Take special precautions for electronic records – monitor access and immediately cut off access to terminated employees.

Keep employee information off of your external Web site – posting employees' names, photos, and contact information on your Web site makes that information accessible. Shred old employee records/information – don't just dispose of it in a general or common waste container. Ensure private waste contractors take adequate protection against theft of records/data.

- Conduct regular scans of your software system for computer viruses that might allow unauthorized access to confidential data.

- Investigate any large downloads of employee information – any downloads of employee data should be pre-authorized.
- Erase hard drives of old company computers before they are sold, donated or borrowed – purchase software that will completely wipe out the hard drive before it leaves your company. (Management Association of Illinois)

Maintaining I-9's: Do's and Don'ts

Don't get sloppy with your I-9 employment eligibility verification forms, even if you figure the feds are too busy looking for terrorists to bother checking your worker documentation.

Yes, the U.S. Citizenship and Immigration Services concentrates more on security-related sites such as airports and water supplies in the wake of Sept. 11, 2001. But it will respond to complaints including those filed by employees bumped from jobs by illegal workers. And penalties can be high: Poor documentation can cost you \$1,000 per worker, and knowingly hiring an illegal alien can result in a \$10,000 per-worker fine.

To sidestep potential legal trouble and discrimination complaints, follow these I-9 do's and don'ts:

Do require all new hires to complete and sign Section 1 on their first day of work.

Don't ask an applicant to complete an I-9 prior to extending a job offer (can lead to claims of discrimination by those not hired)

Do review each employee's documents to make sure they're on the I-9s list of acceptable documents and that they appear genuine (see www.uscis.gov/graphics/formsfee/forms/i-9.htm).

Don't ask new hires for any particular documents or for more documents than the I-9 requires.

Do establish a consistent procedure for completing I-9's and educate your hiring managers.

Don't consider the expiration date of I-9 documentation when making hiring or firing decisions.

Don't forget to keep a tickler file to follow up on expiring documents that limit the employee's authorization to work. You don't have to reverify identification documents, such as driver's licenses.

Do keep I-9's and copies of documents for three years after the employee's hire date or one year after his termination, whichever comes later.

Don't put the Form I-9 in an employee's personnel file. To protect your company against discrimination claims, keep the I-9 and supporting documentation in a separate file.

(The HR Specialist, Employers Association of Florida)

Kurt G. Waldthausen
Waldthausen & Associates, Inc.
KWaldthausen@waldthauseninc.com