

## LAW

### Workplace Identity Theft

## Proactive Measures Minimize Liability

Identity theft is one of the fastest growing crimes in the U.S. There are over seven million identity theft victims each year. A prime target for identity theft is employee sensitive identifying information (EII) maintained by employers. Identity thieves use a variety of methods to gain access to EII, including stealing records from the employer, bribing an employee who has access to these records, or hacking into the employer's computer systems.

Employers should manage EII cautiously and with heightened sensitivity in order to minimize the risk of identity theft. To this end, internal policies and procedures governing the collection, use and protection of EII should be audited. Where such policies and/or procedures are lacking or deficient, new ones should be formulated and implemented, and security measures should be undertaken periodically to evaluate the managing and safeguarding of EII.

Below are steps to be taken to reduce the chances of workplace identity theft and to minimize possible liability. These steps are not, however, intended to be exhaustive. EII management policies and procedures should be customized to meet the needs and legal requirements of employers' specific industries and activities.

**Establish a Policy.** Develop a policy that identifies the circumstances under which sensitive identifying information may be collected from job applicants and employees, the types of information to be collected, and how and when the employer may use and disclose the information.

The policy must comply with applicable federal and state laws governing the security and privacy of EII, including health information. It should limit the collection, use and disclosure of EII to the minimum necessary



Maria Recalde

for its intended purpose. Employers should look, for example, at how and when they collect and use employees' Social Security numbers (SSN) and consider alternative identification descriptors randomly assigned to replace the use of SSNs.

Audit EII currently maintained and determine if all information collected is essential for business or government reporting purposes. Discontinue collecting and properly dispose of any information that is not essential.

#### **Review Record Disposal Policies.**

Outdated hard copy records containing EII should never be merely discarded, but should be shredded internally or by an outside bonded vendor after conducting an appropriate check. Wipe software should be used when disposing of computer files, diskettes, hard drives or any other media where EII was stored.

When applicable, comply with the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requiring the proper destruction of "consumer information" (i.e., any record about an individual, whether in paper, electronic or other form, that is a consumer credit report or is derived from such a report). FACTA requires any person or company that possesses or maintains such information to "tak[e] reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." Businesses must come into compliance by June 1, 2005, by adopting and implementing their own document destruction policies or by contracting with a document/data destruction company to do so.

**Review Computer Systems Security.** Ensure that adequate protective measures are being taken to protect the company computer systems. Keep operating systems

# WOMEN'S BUSINESS<sup>®</sup>

BOSTON

Covering Massachusetts, New Hampshire and Rhode Island

April 2005

THE PROFESSIONAL AND BUSINESS WOMAN'S JOURNAL

security patches current. Update virus protection software regularly. Computer viruses can have damaging effects, including introducing program codes that cause the computer to send out files or other stored information.

In addition, install, maintain and monitor firewalls and intrusion detection systems. Review the company's electronic communications policy to ensure that employees know what policies and procedures they are required to follow to avoid security breaches. Train employees on how they can identify and report possible security breaches.

**Review EII Use by HR Information Systems.** These systems let employers keep track of all employees in a database or in a series of interrelated databases. HRIS includes, among other things, the employee name, SSN, date of birth and contact information. Some HR information systems are interfaced to payroll or other financial systems, all of which are subject to infiltration.

Employers and HR managers must understand the risks of HRIS and take effective steps to secure vulnerable networks, including working with information technology to develop security strategies.

**Restrict Access to EII.** Keep all employee (and job applicant) records in secured areas. Those with access to such records should be clearly identified and should have completed training on identity theft and document handling practices. Responsibilities for maintaining the security of EII should be assigned.

Computers used by employees with access to EII should automatically lock down if unused for a designated period of time. Computer printers and fax machines for employees who use and disclose EII as part of their job functions and responsibilities should be maintained in controlled areas. EII should be encrypted while being

transmitted electronically. Storing EII on laptops or other computers readily available to employees should be avoided.

Background checks should be conducted for all employees who have access to EII. Temporary employees and vendors should be barred from sensitive identifying information, except when absolutely necessary and only after an appropriate background check has been conducted.

**Develop a Contingency Plan.** The contingency plan should address how the company will deal with security breaches internally as well as how to assist affected employees. Employees should be made aware of resources and information available to assist in combating identity theft, such as the FTC's Web site, <http://www.consumer.gov/idtheft>.

**Stay Up to Date.** Keep informed of changes in the law and governmental efforts, at both the federal and state level, that may impact the collection, use, storage and/or disposal by employers of EII.

While the damage to an employer from the unauthorized use of EII could be significant, liability for the damage caused to individual employees when EII is used for fraudulent purposes poses a greater risk. Accordingly, employers need to be proactive in taking preventive measures against workplace identity theft. The appropriate policies and procedures need to be developed, established and implemented in order to reduce potential exposure. Failure to do so may subject employers to costly consequences.

*Maria E. Recalde is a partner at Sheehan Phinney Bass + Green's Boston office. She is a member of the firm's Business Litigation and Intellectual Property and Technology Practice Groups.*