EMPLOYMENT & LABOR ARTICLE

ROBINSON BRADSHAW & HINSON

JUNE 2009

What Employers Need to Know about the North Carolina Identity Theft Protection Act

By Ty E. Shaffer

The North Carolina Identity Theft Protection Act (the ITPA) requires businesses to guard the personal information of their customers and clients. Because personnel files likely contain identifying personal information, the ITPA also governs the maintenance and destruction of employee records. This article outlines the steps employers should take to ensure that their treatment of employee records complies with the ITPA.

Protecting social security numbers and "personal information"

Personnel records likely contain employees' social security numbers, and the ITPA demands that employers treat them with care.

- If employees are required to transmit their social security numbers online, then the connection must be secure or the social security number must be encrypted.
- In addition to security and/or encryption, if employees use their social security numbers to access any employer web sites, they also must be required to use a password, unique personal identification number (PIN), or some other authentication device along with their social security numbers.
- Social security numbers cannot be printed on materials mailed to employees unless it is required by state or federal law.
- Social security numbers cannot be printed or embedded on a card that employees must carry in order to access certain services.

In addition to social security numbers, the ITPA protects against the publication of "personal information." The Act defines "personal information" as the combination of a person's name with, among other things, that person's drivers license number, digital signature, biometric data, or fingerprints. If you publish or broadcast any information about your employees, it is important to be sure that the information you disclose does not violate the ITPA.

Destroying personnel records

The obligation to protect personal information extends to taking reasonable measures to guard against unauthorized access to or use of that information after its disposal. These measures include the destruction of employee records (whether in paper or electronic form) such that personal information cannot be read or reconstructed. In addition, employers must maintain "as official policy in the writings of the business entity" a description of their policies and procedures relating to the proper disposal of personnel records in compliance with the ITPA.

The ITPA does authorize businesses to enter into contracts with document destruction specialists, but only "after due diligence." This due diligence must include one or more of the following actions:

- Reviewing an independent audit of the disposal business' compliance with the ITPA or of its business operations;
- Consulting references or other reliable sources and requiring that the disposal business be certified by a recognized trade association, such as the National Association for Information Destruction ("NAID"), or other entity that provides such certification; or
- Reviewing and evaluating the disposal business' information security policies and procedures, or taking other steps to determine the competence and integrity of the disposal business.

Dealing with security breaches

In addition to the general requirement that businesses make reasonable efforts to protect against a security breach, the ITPA requires businesses to take affirmative steps to notify employees whose personal information is at risk. Specifically, "immediately following the discovery of the breach," an employer must give employees a "clear and conspicuous" notice containing the following information:

- A description of the incident in general terms;
- The type of personal information that may have been accessed;
- A general description of the actions that the employer is taking to protect employees' personal information from further unauthorized access;
- A telephone number that employees may call for more information and assistance; and
- A statement advising employees to remain vigilant by reviewing their account statements and consulting free credit reports.

Consequences of noncompliance

The costs of violating the ITPA may be significant. For example, an employer could face a civil action in which damages will be tripled. In addition, the court may award a successful plaintiff its attorney's fees. The Attorney General also is empowered to institute a suit against a violating party, and the court may impose a civil penalty of $5,000 for each violation of the ITPA.

What steps should employers take to ensure compliance?

- Review your recordkeeping practices. Now is the time to be sure that your recordkeeping practices comply with the ITPA. For example, any paper copies of personnel records should be kept in a secure area, and employers should have a set procedure for review of employee records to ensure that there is

no unauthorized access. Employers also should take this opportunity to ensure that their treatment of employee social security numbers does not violate the ITPA. In addition, if you currently use a document destruction service, find out if it is accredited by the NAID and ask about the steps it takes to guarantee compliance with the ITPA.

• Create and implement a written recordkeeping policy. By developing practices that comply with the ITPA, employers can reduce the risk that personal information will be disclosed or otherwise misused. The ITPA requires employers to adopt a written policy for the destruction of confidential records. But a written records management policy also should describe procedures for accessing and protecting personnel records, as well as procedures for responding to any security breaches.

• Periodically test the security of electronic records. Because electronic records are popular targets for identity theft, employers must be sure that these records are secure from unauthorized access. Regular testing of the security of systems and electronic records will help to prevent security breaches.

• Educate your employees. Employers should ensure that those employees responsible for maintaining (and destroying) personnel records understand their obligations under the ITPA.

The threat of identity theft means we must be increasingly careful in the ways we use information about ourselves and others. Both individuals and business have a role to play in ensuring that personal information remains confidential. The requirements that the ITPA imposes on businesses are common to an array of state statutory schemes designed to protect citizens from identity theft. Because North Carolina's ITPA has counterparts in other states, multi-state employers must be mindful of the demands imposed by the laws of other states where they operate.