

Identity Theft Protection Act Client Alert - 2005

Many North Carolina businesses are not prepared for a series of new legal obligations imposed by the State's new Identity Theft Protection Act (ITPA). The ITPA applies to all companies located or doing business in North Carolina, and most of its key provisions went into effect December 1, 2005. Is your company in compliance?

Identify Theft Is A Risk For Every Business And Employer

The theft of personal information to commit fraud has been cited by the Federal Trade Commission (FTC) as the fastest growing crime in the nation and North Carolina. Perhaps most troubling to businesses is the theft of personal information by corrupt employees. Not only are such cases harmful to the businesses' reputations and costly to manage and rectify, the number of potential victims impacted by such security breaches can be substantial.

However, all employers should take note that the theft of personal information from businesses is *not* limited to consumer or customer information. Indeed, the FTC reported in 2003 that approximately *90% of business record thefts involved payroll or employment records*. This should not be a surprising fact when one takes even a moment to think of the wealth of personal information maintained in company files regarding employees (and their family members), including drivers license numbers, social security numbers, bank account numbers for direct deposit, tax information, retirement account information, and health insurance and medical information.

As our clients in the financial services and health care sectors are well aware, both the federal government and many states are responding to this threat by enacting legislation and promulgating rules designed to make businesses take better care of personal information regarding their customers and employees. For example, in recent years the U.S. Congress has passed the Gramm-Leach-Bliley Act imposing privacy requirements on the financial services industry, and the U.S. Department of Health and Human Services has promulgated privacy and security rules under the Health Insurance Portability & Accountability Act (HIPAA) that apply to many health care providers and health plans. Congress also amended the Fair Credit Reporting Act to strengthen consumers' ability to fight identity theft. This amendment included the "Disposal Rule" which became effective in June 2005, requiring all businesses to use reasonable methods and due diligence to ensure that consumer information is properly destroyed so that criminals cannot recover it from the trash. Now, with ITPA, North Carolina has added another set of regulatory requirements and another potential source of liability for businesses for improperly handling personal information.

Key Provisions Of The North Carolina Identity Theft Protection Act

Considered one of the strongest state identity theft laws in the nation, the ITPA imposes numerous obligations on all employers and businesses in North Carolina to protect personal information. "Personal information" is broadly defined under the ITPA and includes a person's name in combination with identifying information such as social security numbers, drivers license numbers, bank account and credit card numbers, email addresses, PIN codes, and any other numbers or information that can be used to access a person's financial resources. The ITPA is a comprehensive law with three central components of which all businesses should be aware.

First, the ITPA places strict procedures on the use and disclosure of social security numbers. Except for certain legitimate business reasons, effective immediately, businesses cannot intentionally communicate or otherwise make available to the general public an individual's social security number. In addition, businesses should begin preparing for a second set of obligations that will become effective on October 1, 2006. This next phase of the ITPA imposes prohibitions on the use of social security numbers on cards required to access services and products, limits how social security numbers may be used and transmitted on business websites, and regulates how social security numbers should be protected in company mailings.

Second, the ITPA now specifies the steps businesses must take in the event of a security breach, such as the theft or loss of consumer or employee personal information. The ITPA imposes a duty on all businesses to report the breach "without unreasonable delay" to anyone whose information might have been compromised. The ITPA dictates both the content of the notice and how it must be sent. In addition, to mitigate the damage of identity theft, the ITPA permits a person to request a "security freeze" preventing consumer reporting agencies from releasing the person's credit report.

Finally, the ITPA requires all businesses to ensure that personal information of consumers and employees is disposed of in manner that prevents identity thieves from recovering it. All businesses (except certain financial institutions, health care insurers and facilities, and consumer reporting agencies subject to federal law) are required immediately to develop formal written policies and procedures for the disposal of personal information. However, the ITPA makes clear that merely having a policy in a manual is *not* enough. Businesses are required to monitor the policy to make sure their employees are actually complying with it.

In disposing of personal information, the ITPA mandates that all businesses take "reasonable measures" against unauthorized access to the information during and after its disposal. This requirement expressly applies to electronic media and equipment, so businesses should be particularly cautious when discarding, donating or selling used computer equipment to ensure that any personal information stored in the equipment is effectively rendered unreadable and unable to be reconstructed. If a business engages a commercial record disposal or shredding company, the ITPA specifies the "due diligence" steps that the business must conduct *before* entering into a contract with the disposal company.

Violations of the ITPA will subject a business to lawsuits and liability under North Carolina's Unfair and Deceptive Trade Practices Act, including treble damages and attorneys' fees. However, as incentive for businesses to formulate and monitor effective policies, treble damages are not allowed for acts or omissions of non-managerial employees in improperly disposing of personal information, *unless* the business negligently fails to train, supervise or monitor those employees.

2006 Action Items For All North Carolina Businesses

As a result of the ITPA's mandates and stern penalties, we are generally recommending that all of our North Carolina clients act now and, at a minimum, take the following immediate steps to ensure compliance with the new law:

- Conduct a **self-audit** of the security of the information collected on consumers and employees, evaluating whether all of the information collected is truly necessary, determine where it is maintained, whether it is adequately secured, who has access to it, and how it is disposed of.
- Implement a formal **written** policy addressing the security of, access to, and proper disposal of personnel records and consumer data containing personal information. This policy should also address how personal information stored in outdated computer equipment and media is to be destroyed or rendered unreadable.
- **Train employees** on the importance of securing the personal information of employees and consumers, and instruct them on the company's policies and procedures safeguarding that information.
- **Assign a manager** to be responsible for monitoring compliance with the policy, training employees, and ensuring that due diligence is exercised when personal information and personnel records are disposed of or destroyed.
- Develop an **action plan** to handle security breaches that compromise the personal information of consumers or employees, including a mechanism to issue the proper legal notice to those affected "without unreasonable delay."

In addition to these immediate steps, businesses should be aware of the second set of obligations under the ITPA which will become effective in October 2006. These provisions may require updating computer and internet applications and may take some time to prepare for.

The enactment of the ITPA provides North Carolina businesses with the opportunity and the incentive to fully examine their internal security and information handling practices and policies. If you have any questions about this new law or how it affects your current practices and procedures, please contact the attorney with whom you usually work, or contact [John Pueschel](#) by telephone at 336.721.3726 or [email](#).

IRS CIRCULAR 230 NOTICE: *To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (or in any attachment) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed in this communication (or in any attachment).*