



A GUIDE TO THE NORTH CAROLINA IDENTITY THEFT PROTECTION ACT

Identity theft once was a matter left solely to criminal law—prosecuting those who used the personal information of others for financial gain. But the exponential growth of identity theft in recent years has led many states, including North Carolina, to impose new obligations on businesses to protect the privacy of a consumer's personal information.

California enacted the first such law in 2002 after hackers broke into a state payroll database that included the names, social security numbers, and bank account information for over 250,000 state workers. The California law required companies that own or license computerized "personal information" to disclose any breach of security to any consumer whose unencrypted data is believed to have been disclosed.

Since 2002, there has been a virtual avalanche of activity in state legislatures to combat identity theft. A growing list of states followed California's lead and imposed new obligations on businesses to safeguard consumer privacy.

North Carolina has now joined that list.

On September 21, 2005, Governor Easley signed into law the Identity Theft Protection Act of 2005 ("ITPA" or "the Act"). The overarching goal of ITPA is to protect the privacy of a consumer's "personal information." ITPA defines personal information as (1) a consumer's first name or first initial and last name and (2) one or more of the following:

- Social security or employer identification number
- Driver's license, passport, or state identification number
- Checking or savings account number

- Credit or debit card number
- Personal identification (PIN) number
- Digital signatures
- Biometric data
- Fingerprints
- Passwords
- Parent's last name prior to marriage
- Electronic information numbers or electronic mail names or addresses, Internet account numbers, or Internet identification names
- Any other number or information that can be used to access a person's financial resources.

To prevent unauthorized disclosure of personal information, ITPA imposes four new burdens upon businesses:

- Notification of Security Breaches. The Act requires businesses to notify consumers in the event of a security breach of a consumer's personal information—unless the personal information has been encrypted or redacted in a manner that renders the information unusable or unreadable to third parties.
- No Disclosure of Social Security Numbers. Subject to certain specific exceptions, the Act prohibits businesses from disclosing a consumer's social security number ("SSN").

- Destruction of Records Containing Personal Information. The Act requires businesses to either (a) take “reasonable measures” to prevent disclosure of personal information during the destruction of records containing such information, or (b) contract with a third party in the business of destroying personal records.
- Security Freeze. Consumers may request that consumer reporting agencies place a security freeze on their credit reports to prohibit a third party from accessing credit information without written authorization of the consumer. The consumer may request that the freeze be temporarily lifted to permit access to credit information for a specific amount of time.

These multiple obligations on businesses make ITPA one of the most stringent and far-reaching identity theft laws in the United States. ITPA applies to all “businesses”—sole proprietors, partnerships, associations, corporations (including not-for-profit entities), and financial institutions. And the prohibition on disclosure of personal information applies not just to computer information but to *all* forms of personal information—including paper files.

The penalties for noncompliance with ITPA can be severe. Lawsuits brought by the attorney general can result in statutory damages of up to \$5,000 *per violation*—even without any showing of injury to a consumer—if a business knowingly commits a violation of ITPA. Private lawsuits brought by consumers may result in treble damages and attorneys’ fees upon a showing of actual injury. The prospect of class action lawsuits is real.

In light of the new obligations imposed by ITPA, businesses should take special care to establish sufficient internal procedures to protect the privacy of consumers’ personal information. ■

We would be happy to assist you with any of the preceding matters. Please contact one of the following Brooks Pierce advisors if you would like to discuss these issues.

CONTACT INFORMATION

Charles F. Marshall
(919) 573-6247
cmarshall@brookspierce.com

J. Benjamin Davis
(919) 573-6226
jdavis@brookspierce.com

Elizabeth E. Spainhour
(919) 573-6229
espainhour@brookspierce.com

BROOKS, PIERCE, McLENDON, HUMPHREY & LEONARD, LLP

150 Fayetteville Street Mall
1600 Wachovia Capitol Center
Raleigh, NC 27601

WWW.BROOKSPIERCE.COM

Greensboro, NC • Raleigh, NC

Brooks, Pierce, McLendon, Humphrey & Leonard, LLP is a business law firm providing comprehensive strategic counsel and innovative solutions to its clients. The information contained in this bulletin is not legal advice and does not create an attorney-client relationship between the reader and Brooks, Pierce, McLendon, Humphrey & Leonard, LLP.
