North Carolina Identity Theft Protection Act - The Importance of Keeping Private Information Private by Caren D. Enloe

August 1, 2006

In recent years, the number of reports of identity theft has increased dramatically in North Carolina. Personal information, including a social security number, is regularly requested by businesses from their employees and customers for a variety of purposes. Consequently, many of these businesses possess large databases of personal information that are ideal targets of perpetrators of identify fraud. In response to this growing problem, the North Carolina Legislature adopted The Identity Theft Protection Act, with an effective date of December 1, 2005 for the main provisions. The Act affects all companies doing business in North Carolina and imposes upon these specific duties and restrictions regarding the use and maintenance of personal records of their employees and customers. While we provided our clients with an overview of this law in our last issue of Legal Insights, in this issue we offer a more in-depth review of the contents and implications of this bill.

The Identity Theft Protection Act (ITPA) has three main goals:

1. to prevent personal information of individuals from falling into unauthorized hands by imposing specific regulations on businesses
2. to require businesses to properly dispose of all personal information of their customers and employees
3. to require businesses to provide adequate notice of a security breach to any affected party upon discovery that personal information has been either lost or stolen

The ITPA's intent is to protect the personal information of those individuals identified as either consumers or employees of a business. This includes any combination of a person's name and another personal identifier, including social security number, PIN number, driver's license number or bank account number.

Businesses Must Take Affirmative Steps to Prevent Disclosure of Personal Information

The ITPA prohibits businesses from intentionally communicating or otherwise making available to the general public an individual's social security number, aside from its last four digits. As such, a business that uses a social security number as a means of identification of an employee or customer must make

sure that it eliminates any possibility of unintended dissemination of the personal identifier. Specifically, a company doing business in North Carolina cannot:

1. intentionally print an individual's social security number on any card required for access to products or services
2. require an individual to transmit his or her social security number over the internet, unless the connection is secure
3. require an individual to transmit a social security number to access an internet website, unless a password is also required
4. print an individual's social security number that may be visible on any mailed materials
5. sell, lease, loan, trade, rent, or otherwise intentionally disclose an individual's social security number to a third party without written consent

A few exceptions, however, allow a business to use a social security number for limited purposes. The prohibitions do not apply when the social security number is:

1. included in an application
2. used for internal verification and administrative purposes
3. used to open an account
4. used to investigate fraud, conduct background checks, collect debts, obtain credit reports, furnish information to a reporting agency, or locate an individual
5. produced pursuant to a court order or valid subpoena.

Affirmative Steps to Destroy All Personal Information

The ITPA imposes on businesses a duty to take all reasonable measures to properly dispose of all personal information of consumers in order to prevent any unauthorized use of the information during and after its disposal. All businesses have a duty not only to implement but also to monitor formal policies and procedures that require proper disposal of all personal information. The Act also imposes a duty to destroy any data located in electronic media. Businesses have the option to employ a commercial record disposal company in order to ensure that proper disposal of personal information is performed. A commercial record disposal company will help a business ensure that the personal information is properly and adequately disposed, preventing any opportunity for unlawful dissemination of the same. However, since

the disposal of personal information must be done in strict compliance with the Act, before a business can enter into a written contract with a disposal company, it must first exercise "due diligence" in selecting and evaluating said company to ensure that it will, in fact, adopt appropriate measures.

In Case of a Breach, What Must A Business Do?

If a business becomes aware of a security breach (for example, if information has been lost or stolen), the Act obligates the business to give notice "without unreasonable delay" to the affected party whose personal information may have been compromised. The notice must be clear and conspicuous and its content must specifically adhere to the requirements delineated in the Act. Furthermore, the notice must be provided by one of the methods specified, by telephone, written correspondence, or email.

Are Damages Assessed In The Case of A Violation?

Yes. A violation of the Act can result in significant damages if it is found that the business was negligent in developing and monitoring its disposal policies and training and supervising its employees, or was willful in allowing personal information to be lost or stolen.

How Can A Business Ensure Compliance With The Requirements And Duties Imposed By The Identity Theft Protection Act?

There are three primary actions a business in North Carolina should take in order to ensure compliance with the ITPA. First, the business should perform an initial assessment of its current measures and procedures employed to protect personal information of its consumers and employees to determine whether they are in compliance. Then, a formal written policy should be developed and implemented which details the proper procedure for disposal of all personal information, and all employees should be properly trained accordingly. And lastly, the business should develop a strategy for storing personal information in a manner that safeguards it. This policy should also address the protocol for dealing with possible breaches, including plans for proper notice to any affected individual.