

What is the New Jersey Identity Theft Prevention Act?

New Jersey's Identity Theft Prevention Act (ITPA) protects individuals from identity theft in various ways, including: requiring consumer credit reporting agencies to place security freezes on consumer reports upon request; requiring businesses that collect digital records containing personal information to notify individuals whose personal data is compromised; limiting the use of Social Security numbers as general identifiers; and requiring businesses to destroy personal information that is no longer needed. ITPA came into force on January 1, 2006.

Who is affected?

ITPA applies to all businesses that operate in New Jersey or who collect and store personal information about New Jersey residents. "Personal Information" is defined as non-public, unencrypted information consisting of an individual's first name or first initial and last name linked with any one or more of the following: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Certain publicly-available information is exempted.

What does the ITPA have to do with information management?

Sections 10 through 15 of ITPA deal with the security of personal information. Section 11 states:

A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.

What do companies have to do to comply with ITPA?

Businesses must alert affected customers when personal information which is not publicly available is acquired, or is thought to have been acquired, by unauthorized parties. Methods for notifying affected individuals are outlined in the Act. If the cost of notifying affected individuals is more than \$250,000 or the number of affected individuals exceeds 500,000, substitute notification methods may be followed.

Additionally, businesses that experience a security breach of more than 1,000 personal records at a time must contact all consumer reporting agencies that compile and maintain consumer records on a nationwide basis to notify them of the breach.

It is an unlawful practice to willfully, knowingly or recklessly violate ITPA's personal information security provisions. Businesses must therefore ensure that they securely destroy customers' personal information which is no longer required, as well as disclose computer security breaches and limit the use and disclosure of SSNs.

How can we help?

As you develop your information management program in compliance with the Identity Theft Prevention Act, consider contracting Securit to handle your document destruction needs. Securit securely destroys all your confidential materials, including computerized data. By providing locked consoles for your business, Securit makes it easy and efficient to destroy unnecessary copies of your customers' personal information. Employees place materials to be destroyed in locked boxes which are picked up and shredded. Securit's Certificate of Destruction is your record of the secure destruction process. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

New Jersey Office of the Attorney General, Department of Law & Public Safety,
Division of Consumer Affairs -

<http://www.state.nj.us/lps/ca/home.htm>

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2006

