

New Jersey Employers Must Take Steps To Prevent Identity Theft

Wendy Johnson Lario
and Kimberly A. O'Sullivan

PITNEY HARDIN LLP

On January 1, 2006, the New Jersey Identity Theft Prevention Act ("ITPA") will take effect. The ITPA is a broad state law that sets a new standard in identity theft prevention. The law gives New Jersey residents the power to control access to their consumer reports with a "security freeze." For employers, the ITPA imposes new requirements for the destruction of documents containing personal information, the use and display of social security numbers, and the actions required in the event of unauthorized access to personal information. The ITPA is a consumer-focused law that will have far-reaching implications outside the workplace. However, the law will also have an impact on employer obligations inside the workplace.

Background

The ITPA amends the New Jersey Fair Credit Reporting Act, which imposes disclosure and notice requirements on employers that obtain consumer reports, from third parties, for employment purposes. Prior to enactment of the ITPA, the New Jersey Fair Credit Reporting Act mirrored its federal counterpart. The ITPA, however, now takes the New Jersey law beyond the protections of the federal Fair Credit Reporting Act ("FCRA") and its amendments contained in the federal Fair and Accurate Credit Transactions Act of 2003 ("FACT" Act). The ITPA is a strong response to the rise in identity crimes and the increasing public concern for identity theft.

Destruction Of Personal Information

One provision of the ITPA requires "businesses" to destroy, or arrange for the destruction of, "customer" records within its custody or control, that contain personal information. The records must be destroyed by shredding, erasing, or otherwise modifying the personal information to make it unreadable, undecipherable or nonreconstructable.

This destruction provision creates a sweeping obligation for employers due to its broadly defined terms. "Customer" is defined as an "individual who provides personal information to a business" and "business" is defined comprehensively as "a sole proprietorship, partnership, corporation, association, or other entity." This provision therefore pertains to all New Jersey employers, regardless of size, and all job applicants, contractors, consultants, employees, and agents who provide personal information to them.

Additionally, the term "records" means any "material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted." In other words, all paper and electronic media are covered. Finally, "personal information" includes an individual's first name, or first initial, and last name combined 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



Wendy Johnson Lario

number of credit or debit card number in combination with any required security code, access code or password permitting access to an individual's financial account.

This is the kind of information typically solicited on most employment applications, benefits documents, tax forms, and other employment-related records.

The result of these vast definitions is that both small and large organizations must now destroy personal information relating to applicants, employees and other agents in accordance with the ITPA. Not only must the paper documents be destroyed, but any electronic record or image of such documents must also be completely erased. One silver lining to the ITPA is that there are no guidelines or time requirements for the destruction of such records. Rather, they are to be destroyed when they are "no longer to be retained." Thus, employers may retain these personal records as long as required by any federal, state or local statute, regulation or statute of limitations. In addition, if the records are or may be involved in litigation or an agency charge, they should be retained until the litigation or charge is resolved.

Notably, the destruction provision of the ITPA is similar to the "Disposal Rule," a part of the federal FACT Act that calls for the proper disposal of information contained in or derived from consumer reports. The Disposal Rule became effective June 1, 2005 and applies to all employers that use consumer reports, obtained from third parties, for employment purposes. The definitions in the ITPA, however, are more expansive than the federal Disposal Rule. The principal difference is that the Disposal Rule applies only to personal information contained in or derived from a consumer report. The ITPA pertains to all records containing "personal information," regardless of the source.

Unauthorized Access To Information

The ITPA also requires any "business" that compiles or maintains computerized records that contain "personal information" to disclose to a "customer" any breach of security of those computerized records. The definitions of "customer," "business," and "personal information" are the same broad definitions as described above and apply to all employers and their applicants, employees and other agents.

Further, "breach of security" is defined as unauthorized access to personal information that compromises the "security, confidentiality, or integrity" of the personal information. An important exception to this definition exists for employees of a business who, in good faith and for a legitimate business purpose, acquire personal information. However, such employees may not use the personal information for any other purpose



Kimberly A. O'Sullivan

or subject it to any unauthorized disclosure. In light of these requirements, employers must maintain computerized personal information on secure networks, databases and files. Employers should also restrict access to computer records that contain personal information to certain employees who have been trained on the requirements of this law.

Should a breach of security occur, the ITPA requires employers to disclose the breach to applicants, employees or other agents whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. Thus, if any file, database, or other electronic employment record containing employee names and social security numbers is compromised, the employees must be advised. The law requires that they be advised in the "most expedient time possible and without unreasonable delay."

The requisite disclosure, or notice, may be provided in any one of a number of methods, including written, electronic, or e-mail notice or a conspicuous posting on the Internet web site page of the business, if one is maintained. Additionally, if a disclosure to more than 1,000 persons at one time must be made, the business must also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain records on consumers on a nationwide basis of the timing, distribution and content of the disclosure. However, if employers do not believe that misuse of compromised personal information is reasonably possible, an employer is not required to disclose the security breach to employees or consumer reporting agencies. In those instances, the employer would be obligated to document its determination that misuse was not reasonably possible and retain such documentation for five years.

The Use Of Social Security Numbers

The ITPA further prohibits certain actions relating to the use of social security numbers. Specifically, the ITPA proscribes any "person, including any public or private entity" from:

- Publicly posting or displaying an individual's social security number or any four or more consecutive numbers taken from an individual's social security number;
- Printing an individual's social security number on any materials that are mailed to the individual (unless state or federal law requires the social security number be on the mailed document);
- Printing an individual's social security number on any card required for the individual to access products or services provided by the entity;
- Intentionally communicating or otherwise making available to the general public an individual's social security number;

- Requiring an individual to transmit their social security number over the Internet, unless the connection is secure or the social security number encrypted;

- Requiring an individual to use their social security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access that web site.

Under the Act, "private entity" is broadly defined as "any individual, corporation, company, partnership, firm, association, or other entity, other than a public entity." Accordingly, all employers fall within the scope of this definition. Employers should be aware of these new requirements, particularly if they use a web site to process job applications that solicit a candidate's social security number. Employers should also check to ensure that social security numbers are not displayed on employee identification or health insurance cards. Additionally, employers should not issue any mail where social security numbers are visible through an envelope or printed on a post card.

The Security Freeze

The ITPA supplements the New Jersey Fair Credit Reporting Act by providing consumers with the opportunity to implement a "security freeze." When a consumer requests a security freeze, consumer reporting agencies are prohibited from releasing the consumer report, or any information from it, without the express authorization of the consumer.

The IPTA allows a consumer to temporarily lift the freeze, either for a specific business or a certain period of time. Once the freeze is lifted, consumer reporting agencies have three business days to issue the information. The security freeze is similar to the fraud alert that consumers can place in their consumer reports pursuant to the federal FCRA. However, under the IPTA, all consumers can implement a security freeze, whereas under the FCRA, fraud alerts are permitted only if there has been an incident or alleged incident of identity theft.

Although the security freeze provision of the ITPA does not place any affirmative obligations upon employers, it will likely create more difficulty in obtaining personal information about certain job applicants and employees. Employers may be confronted with situations where personal information cannot be obtained from a job applicant or employee because of a security freeze. If that occurs, employers may request that the individual lift the freeze so that information can be obtained for employment purposes. However, employers should anticipate, and be prepared to tolerate, delays associated with obtaining personal information from a file that has a security freeze in place.

What Should Employers Do?

The ITPA is a broad law that requires employers to take new steps to limit access to records containing personal information and maintain additional destruction procedures for that information. Employers are encouraged to contact legal counsel to assist in reviewing existing hiring procedures and document destruction policies to ensure compliance with the ITPA and its federal counterparts. Indeed, employers must address the destruction of paper records, as well as electronic files and images. Employers should also remember that the ITPA applies not only to the personal information of job applicants and employees, but to temporary staff, consultants and independent contractors. Now is the time to act so that any necessary changes may be implemented, and employees trained, before the new law becomes effective on January 1, 2006.

Wendy Johnson Lario is a Partner and Kimberly A. O'Sullivan is an Associate in the Labor, Employment & Benefits Group of Pitney Hardin LLP. This article represents only the authors' opinions and does not necessarily reflect the views of Pitney Hardin or any of its clients. Ms. Lario and Ms. Sullivan may be reached at (973) 966-6300.

Please email the authors at wlario@pitneyhardin.com or ko'sullivan@pitneyhardin.com with questions about this article.