VEDDERPRICE

# Labor Law Bulletin

Labor and employment law trends of interest to our clients and other friends.

January 2006

## New Jersey Identity Theft Prevention Act Takes Effect January 1

***Significant Effect on Record Keeping, Application Forms and Personnel Practices***

New Jersey's Identity Theft Prevention Act (ITPA), effective January 1, 2006, creates new responsibilities for employers regarding the handling and disposal of personal information received from employees and other individuals. Specifically, the ITPA (1) imposes a duty to destroy records that contain personal information and that are no longer to be retained, (2) imposes a duty to disclose unauthorized access to personal information to New Jersey police and to those individuals whose personal information may have been accessed, and (3) controls employers' display and use of Social Security numbers. Additionally, the ITPA provides an individual with the ability to implement a "security freeze," thereby limiting third-party access to his or her consumer reports.

***What the ITPA Covers***

At first glance, the ITPA seems to apply only to information received from a customer. The law requires a business to destroy certain "customer's records" no longer to be retained by it and, under certain circumstances, to provide notice to a "customer" in the event of unauthorized access to that "customer's" personal information. However, the ITPA's definitions of "customer" and "business" are extremely broad. "Customer" is defined as "an individual who provides personal information to a business," and "business" is defined as "a sole proprietorship, partnership, corporation, association, or other entity." Therefore, the ITPA almost certainly applies to all employers—no matter what size or form—and creates duties relating to personal information received from employees, contractors, agents, consultants, and any other individual.

The ITPA defines "records" to be "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," and defines "personal information" to be "an individual's first name or first initial and last name linked with any one or more of the following data elements: (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." Therefore, the statute applies to such materials as employment applications, benefits forms, tax forms, and other employment-related documents that contain "personal information."

***Destruction of Records Containing "Personal Information"***

The ITPA requires that a "business" destroy a "customer's records" that contain personal information and that the business does not retain. In other words, while the ITPA does not create any affirmative obligations regarding record retention *per se*—such as those imposed by other statutes and regulations—it does impose an obligation once the

retention period ends. Specifically, the business must "destroy, or arrange for the destruction of . . . [the records] by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means."

***Reporting and Disclosure of Security Breaches***

The ITPA also requires a "business" that compiles or maintains computerized records that contain "personal information" to disclose any "breach of security" of those computerized records to a "customer" whose "personal information" may have been accessed by an unauthorized person. The statute defines "breach of security" as "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable." Disclosure must be made to "any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person." However, a business is excused from providing disclosure if the business determines that, despite the breach of security, misuse of the information accessed is not "reasonably possible." This determination must be documented in writing and retained for five years.

If the duty to disclose is triggered, the business must first notify New Jersey's Division of State Police about the breach. The State Police may then notify other law enforcement agencies. If a law enforcement agency determines that disclosure to "customers" will impede an investigation of the incident, disclosure must be delayed until the law enforcement agency notifies the business otherwise. In all other circumstances, after notice to the State Police, the business must provide disclosure to customers "in the most expedient time possible and without unreasonable delay."

The ITPA provides three permissible means by which a business may make the requisite disclosure: written notice, electronic notice, and "substitute notice." A business may provide "substitute notice" in lieu of written notice or electronic notice only "if the business . . . demonstrates that the cost of providing notice would exceed $250,000, or that the affected class consists of subject persons to be notified exceeds 500,000, or the business . . . does not have sufficient contact information." "Substitute notice" consists of the following: "(a) E-mail notice when the business . . . has an e-mail address; (b) Conspicuous posting of the notice on the Internet web site page of the business . . . , if the business . . . maintains one; and (c) Notification to major Statewide media." Additionally, if a business "discovers circumstances requiring notification . . . of more than 1,000 persons at one time," it must disclose the timing, distribution and content of the notices to "all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis."

***Restrictions on Use of Social Security Numbers***

The ITPA prohibits certain conduct in connection with the use of Social Security numbers. Specifically, the statute prohibits any person or business from:

- Publicly posting or publicly displaying an individual's Social Security number, or any four or more consecutive numbers taken from the 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 to be on the document to be mailed;
- 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 his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; and
- Requiring an individual to use his 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 the Internet Web site.

Employers (as well as businesses in general) must be aware of the foregoing prohibitions and should examine their practices to ensure that they will not be in violation of them. For example, an employer in New Jersey that uses an Internet Web site to receive job applications that include an applicant's Social Security number must provide adequate security measures for transmission and receipt as well as maintenance and destruction of that information.

***Availability of a "Security Freeze"***

Employers should also be aware that the ITPA provides individuals with the ability to require consumer reporting agencies to implement a "security freeze." A security freeze "prohibits the consumer reporting agency from releasing [a] report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer report." The "security freeze" therefore may limit the ability of employers to obtain promptly certain information regarding job applicants and employees. So long as a "security freeze" is in effect with respect to an individual, an employer may not obtain personal information from consumer reporting agencies without the individual's express permission. While an employer may request and be granted permission by the individual, this process may delay receipt of requested information.

If you have any questions about the Identify Theft Prevention Act or any other issue, please contact Alan M. Koral (212/407-7750) or any other Vedder Price attorney with whom you have worked.

## VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

Vedder, Price, Kaufman & Kammholz, P.C. is a national, full-service law firm with approximately 225 attorneys in Chicago, New York City and New Jersey. The firm combines broad, diversified legal experience with particular strengths in labor and employment law and litigation, employee benefits and executive compensation law, occupational safety and health, general litigation, corporate and business law, commercial finance, financial institutions, environmental law, securities, investment management, tax, real estate, intellectual property, estate planning and administration, health care, trade and professional association and not-for-profit law.



Questions or comments concerning the Bulletin or its contents may be directed to its Editor, **James S. Petrie** (312/609-7660), or the firm's Labor Practice Leader, **Bruce R. Alper** (312/609-7890), or the Managing Shareholder of the firm's New York office, **Neal I. Korval** (212/407-7780), or, in New Jersey, **John E. Bradley** (973/597-1100).

*Chicago*
222 North LaSalle Street
Chicago, Illinois 60601
312/609-7500
Fax: 312/609-5005

*New York*
805 Third Avenue
New York, New York 10022
212/407-7700
Fax: 212/407-7799

*New Jersey*
Five Becker Farm Road
Roseland, New Jersey 07068
973/597-1100
Fax: 973/597-9607