NEW YORK'S NEW YEAR'S RESOLUTION: PROTECT SOCIAL SECURITY NUMBERS

Labor & Employment Alert
January 2008

Effective immediately, New York's Social Security Number Protection Law imposes new restrictions on the use and display of an individual's Social Security Number (SSN) by individuals and businesses. The law applies to the use of SSNs and any number derived therefrom. Thus, individuals and businesses should be aware that using any part of a SSN, or a number that is obtained from a SSN, exposes them to potential liability under this law. The penalties for violation are swift and substantial.

Individuals and businesses that deal with SSNs should thoroughly review their current policies and procedures regarding the collection and maintenance of SSNs. Businesses should encrypt all SSNs that they transmit or store electronically, and they should ensure that access to SSNs in their possession is strictly limited.

Prohibited Conduct
The Social Security Number Protection Law prohibits individuals and businesses from engaging in the following conduct:

- Intentionally making an individual's SSN available to the public.
- Printing an individual's SSN on any card or tag required for the individual to access products, services, or benefits. (Common examples include membership cards issued by healthcare providers and employee identification or buildingaccess cards.)
- Requiring an individual to transmit his or her SSN over the internet unless the connection is secure or the SSN is encrypted.
- The statute does not define "encrypted" or "secure connection." Consequently, individuals and businesses should ensure that their encryption and security protocols meet or exceed current industry standards.
- Requiring an individual to use his or her SSN to access a Web site, unless a password or unique personal identification number or other authentication device is also required to access the Web site.
- Businesses cannot use an individual's SSN, or SSN derivative, as the sole means for internet authentication. If a business decides to require a SSN for

Attorneys

Joseph Braccio

Peter Godfrey

John Godwin

Practices & Industries

Labor & Employment

authentication to access its website, it must also use a unique password, personal identification number, or similar authentication tool to verify the identity of the user.

- Printing an individual's SSN on any materials mailed to the individual unless required by federal or state law.
- Although the statute places a blanket prohibition on mailing material printed with an individual's SSN, numerous exceptions apply. SSNs may be included in applications and forms sent by mail, provided that the document containing the SSN is sealed in an opaque envelope. The statute provides a non-exhaustive list of documents that qualify as applications and forms, including those sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of a SSN.

Exceptions

The Social Security Number Protection Law explicitly excludes all "encrypted" SSNs from its reach. Thus, individuals and businesses that encrypt SSNs have already taken a large step towards complying with the law.

The law also exempts the collection, use, and release of a SSN as required by federal or state law, for internal verification, fraud investigation or administrative purposes or for any business function authorized by the Gramm-Leach-Bliley Act (15 U.S.C. § 6802). Thus, if a union is able to demonstrate its entitlement to employee SSNs under the National Labor Relations Act, an employer may provide the union with the requested information without violating the Social Security Number Protection Law.

Lastly, the law provides a safe harbor for individuals and businesses that, in good faith, implement policies and procedures to comply with the law. The statute provides that no individual or business will be found in violation of the law if it can show "that the violation was not intentional and resulted from a bona fide error made notwithstanding the maintenance of procedures reasonably adopted to avoid such error."

Access Restrictions

Individuals and businesses are also required to adopt reasonable measures to limit access to SSNs in their possession. Specifically, access to SSNs must be limited to those who have a legitimate or necessary purpose related to the conduct of the business. The law does not define or give examples of what constitutes reasonable measures, but businesses should endeavor to keep access to SSNs to an absolute minimum (i.e., a need-to-know basis).

Penalties

If an individual or business is a first time violator of the Social Security Number Protection Law, a court may impose a civil penalty of up to $1,000 per violation, and up to $100,000 for multiple violations. For repeat offenders, a court may impose a civil penalty of $5,000 for a single violation, and up to $250,000 for multiple violations. The Attorney General is authorized to apply for an injunction upon only five days notice. The law allows a court to issue an injunction without requiring proof that any person has been injured or damaged.

Reminder To Employers

NEW YORK'S NEW YEAR'S RESOLUTION: PROTECT SOCIAL SECURITY NUMBERS

Under the Disposal of Personal Records Act, all New York employers are required to properly dispose of any employee record containing personal information. The law defines personal information as any information that could identify an individual, such as his or her name, SSN, driver's license number, identification card number, mother's maiden name, financial account number or codes, or personal identification number. To properly dispose of a record that contains such personal information, an employer must do one of the following:

1. shred the record;

2. destroy the personal information contained in the record;

3. modify the record so that the personal information is unreadable; or

4. take action consistent with commonly accepted industry practices that the employer reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record.