SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo®

New York Employers Face Penalties if They Fail to Secure Employee Social Security Numbers

Earlier this year, New York joined the growing list of states to adopt legislation that instructs employers and businesses alike to limit their collection and use of employee or customer social security numbers in order to keep this information from being carelessly or intentionally accessed for unlawful purposes.

The new law, like others passed in recent years, is largely in response to the burgeoning problem of identity theft. Although only recognized as a crime since 1998, its incident rate has soared. The Federal Trade Commission (FTC), which began tracking the incidence of identity theft in 1999, reported in its most recent survey that 3.7% of those surveyed were victims of identity theft in 2005, which was equal to 8.3 million U.S. victims.

What some employers may not realize is that the incidence of identity theft in the workplace is a real and growing problem. In a 2006 survey conducted by the Identity Theft Resource Center (ITRC), a not-for-profit organization which provides information and support to identity theft victims, 12% of those surveyed reported that their personal information had been stolen at the workplace. According to the survey, the workplace was the second most common source of stolen information. When the ITRC conducted the survey in 2004, only 1.5% reported that their personal information had been stolen at the workplace. The most frequently reported source of stolen information (41%) was from a person's friend or family member.

The New York law, called the Social Security Number Protection Law, NY Gen. Bus. § 399-dd, specifies what an employer or business can and cannot do vis-a-vis an employee's or customer's social security number and includes monetary penalties for those who violate the section. The law prohibits employers from doing the following:

- Intentionally communicating an employee's social security number to "the general public or otherwise make [it] available to the general public";
- Printing an employee's social security number on any card or tag required to access services or benefits provided by the employer;
- Requiring an employee to transmit his or her social security number over the internet *unless* "the connection is secure or the social security account number is encrypted";
- Requiring an employee to use his or her 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 website";

- Printing an employee's social security number on any materials to be mailed *unless* state or federal law requires that this information be on the document.

In addition to the exceptions noted above, the law expressly provides that social security numbers may be included in mailed applications and forms 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 the social security number. Additionally, the provision does not prevent the "collection, use, or release" of a social security number where required by state or federal law or "internal verification, fraud investigation or administrative purposes or for any business function specifically authorized by 15 U.S.C. 6802 [disclosures made by a financial institution]." Any mailing which contains an employee's social security number must be enclosed in an envelope. No portion of an employee's social security number may be printed on a postcard or other mailing not enclosed in an envelope. The law also provides for notification requirements where information is improperly released.

Although the law provides that employers must take "reasonable measures" to ensure that access to employee social security number information only occurs for "legitimate or necessary purpose[s]," it does not describe what those "reasonable measures" consist of. The following is a list of safeguards employers should take under the guise of "reasonable measures":

- Have a written privacy policy (that includes disposal procedures that are consistent with accepted industry practice and satisfy legal requirements);
- Lock up and limit access to employee personal information;
- Conduct background checks on employees who will have access to personal information;
- Limit retention of personal information to only that which is essential;
- Train employees on privacy and document disposal policies;
- Encourage employees to report any possible security breaches;
- Avoid using or disclosing an employee's social security number for any purpose other than that required by law or legitimate and necessary business purpose; and
- Take proper security precautions when terminating employees who have access to personal information (e.g., changing computer access codes).

How employers dispose of employee personal data is just as important as how employers maintain and secure such information. Since the end of 2006, New York employers have had to comply with the state's Disposal of Personal Records Law, NY Gen. Bus. § 399-h, which mandates how employee personal records should be disposed of. This law piggybacked a 2005 FTC rule, which addressed the proper disposal of sensitive personal consumer information contained in a consumer report.

The New York law provides that documents containing personal identifying information (e.g. social security numbers) may not be disposed of unless: 1) the document is shredded prior to disposal; 2) the personal identifying information is destroyed; 3) the personal identifying information is modified in order to make it unreadable; or 4) some action is taken that is "consistent with commonly

accepted industry practices . . . [that] will ensure that no unauthorized person will have access to the personal identifying information contained in the record."

Employers are subject to civil monetary penalties under both §§ 399-dd and 399-h. First time violators of § 399-dd are subject to up to $1,000 for a single violation and up to $100,000 for multiple violations resulting from a single act or incident. For any subsequent violations of this provision, violators are subject to up to $5,000 for a single violation and up to $250,000 for multiple violations resulting from a single act or incident. Violators of the state's records disposal provision are subject to up to $5,000 per violation and may face additional liability in the event the employer's negligent disposal of records results in a case of identity theft.

If you have any questions regarding this One Minute Memo, please contact the Seyfarth Shaw attorney with whom you work, or any Labor & Employment attorney on our website, www.seyfarth.com.