



HOUSE COUNSEL

DECEMBER 2009

**STATE SOCIAL SECURITY
NUMBER LAWS
AND REQUIRED
POLICIES
— WHO KNEW?**



By **Melissa J. Krasnow**

Businesses possess a great deal of personal information about job applicants, employees, and former employees (e.g., retirees). In addition, employees and independent contractors of businesses often have access to personal information. One of the most common types of personal information is a Social Security number.



**Melissa J.
Krasnow**

In addition to the 45 state data breach notification laws (Minnesota has one) that cover names plus Social Security numbers and address the no-

tification a company must make in the event of a data breach, there are at least 30 lesser-known state laws (Minnesota has one) that cover Social Security numbers. Five of these state laws — Connecticut, Michigan, New Mexico, New York and Texas — require businesses to have a written Social Security number policy.

This article provides a brief overview of the varying policy

requirements and enforcement of these laws.

Connecticut. A business that collects Social Security numbers in the course of business must create a published or publicly displayed (e.g., posting on an Internet Web page) privacy protection policy that: (i) protects the confidentiality of Social Security numbers, (ii) prohibits unlawful disclosure of Social Security numbers and (iii) limits access to Social Security numbers. There is a civil penalty of \$500 for each intentional violation, up to \$500,000 for any single event. **1**

Michigan. A business that obtains Social Security numbers in the ordinary course of business must create a privacy policy that: (i) ensures, to the extent practicable, the confidentiality of the Social Security numbers, (ii) prohibits unlawful disclosure of the Social Security numbers, (iii) limits who has access to the information or documents containing the Social Security numbers, (iv) describes how to properly dispose of documents containing the Social Security numbers and (v) establishes penalties for violation of the policy. This policy that must be published in an employee handbook, procedures manual or in similar documents, which may be made available electronically. This privacy policy requirement does not apply to a business that possesses Social Security numbers in the ordinary course of business and in compliance with the federal Fair Credit Reporting Act or the federal Gramm-Leach-Bliley Act. **2**

New Mexico. A business acquiring or using Social Security numbers of consumers must adopt internal policies that (i) limit access to the Social Security numbers to those employees authorized to have access to that information to perform their duties and (ii) hold employees responsible if the

Social Security numbers are released to unauthorized persons. **3**

New York. An employer must not, unless otherwise required by law: (i) publicly post or display an employee's Social Security number; (ii) visibly print a Social Security number on any identification badge or card, including time card; (iii) place a Social Security number in files with unrestricted access or (iv) communicate an employee's personal identifying information to the general public. "Personal identifying information" means Social Security number, home address or telephone number, personal e-mail address, Internet identification name or password, parent's surname prior to marriage or driver's license number. There is a civil penalty of up to \$500 on an employer for any knowing violation of the law. A violation will be presumed to be "knowing" if an employer has not put in place any policies or procedures to safeguard against such a violation, including procedures to notify relevant employees of the law. **4**

Texas. A business may not require an individual to disclose the individual's Social Security number to obtain goods or services from or enter into a business transaction with a person unless the business: (i) adopts a privacy policy, (ii) makes the policy available to the individual and (iii) maintains under the policy the confidentiality and security of the Social Security number disclosed to the business. This policy must include: (a) how personal information is collected, (b) how and when personal information is used, (c) how personal information is protected, (d) who has access to personal information and (e) the method of disposal of personal information. There is a civil penalty of up to \$500 per calendar month during which a violation occurs (one per month). In addition, the Texas Attorney General may

pursue an action for injunctive relief. Finally, the privacy policy requirement does not apply to (1) a business that is required to maintain and disseminate a privacy policy under the federal Gramm-Leach-Bliley Act, (2) the federal Family Educational Rights and Privacy Act or the Health Insurance Portability and Accountability Act of 1996, (3) a covered entity under rules of the Texas commissioner of insurance relating to insurance consumer health information privacy or insurance consumer financial information privacy, (4) a governmental body other than a municipally owned utility or (5) a business with respect to a loan transaction if the business is not engaged in the business of making loans. **5**

Even if a business is not subject to the Connecticut, Michigan, New Mexico, New York or Texas laws, it should determine whether it is subject to other state Social Security number laws. One way of facilitating compliance with such laws is through a written policy regarding the use of Social Security numbers. ■

Melissa Krasnow is a partner in the corporate group of Dorsey & Whitney LLP's Minneapolis office.

FOOTNOTES

- 1 Conn. Gen. Stat. sec. 42-471
- 2 Mich. Comp. Laws sec. 445.84
- 3 N.M. Stat. sec. 57-12B-3
- 4 N.Y. Lab. Law sec. 203-d
- 5 Tex. Bus. and Comm. Code secs. 501.051-053

Reprinted with permission of
Minnesota Lawyer.

For subscription information,
please call 800-451-9998.

MINNESOTA LAWYER