Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=da627d01-2b49-4239-9852-26274f107e74

MORRISON | FOERSTER

Legal Updates & News

Bulletins

Six States Now Require Social Security Number Protection Policies

December 2008
by Miriam Wugmeister, Nathan D. Taylor

Related Practices:

- Employment and Labor
- Financial Services Law
- Privacy and Data Security

Privacy and Data Security Update, December 9, 2008

More than 30 states have adopted laws limiting how Social Security numbers ("SSNs") can be collected, used, and disclosed. Six of those states have adopted provisions that specifically require organizations to develop policies to safeguard SSNs. It is important to keep in mind that a business may collect SSNs not only from its customers, but also from its employees or small vendors who use SSNs as their Tax ID number. As a result, almost every business needs to be aware of these state laws and, where applicable, take steps to comply with them.

Over the past five years, the issue of data security has received heightened legislative scrutiny, particularly at the state level. The principal focus of this scrutiny has been the extent to which organizations maintain the security of sensitive personal information relating to their customers, their employees, and other individuals. As a result, the states have actively regulated how and when organizations must protect personal information. From breach notification laws to laws placing specific obligations on how organizations are to safeguard personal information to avoid its unintended disclosure, the states have been and continue to be at the forefront of data security legislation. For example, at least 44 states, as well as the District of Columbia and Puerto Rico, have enacted laws imposing some form of notification obligation on an organization that learns of an unauthorized access to, or acquisition of, personal information.[1]

The states have also focused on enacting underlying requirements for how a business must maintain the security of specific types of information. United States legislation at both the federal and state levels has focused on preventing harm and misuse of personal information. Thus, not surprisingly, the initial focus of states has been on what is considered to be the personal information most likely to be used to harm individuals, namely, SSNs. At least 31 states have adopted laws restricting or prohibiting the collection, use, or disclosure of SSNs.

Six states in particular - Connecticut,[2] Massachusetts,[3] Michigan,[4] New Mexico,[5] New York,[6] and Texas[7] - have enacted laws or regulations that require organizations that collect or use SSNs to implement policies to protect those SSNs and, in some instances, to make their SSN protection policies available to the public or to their employees. In many respects, these state SSN protection policy requirements are similar to the federal Gramm-Leach-Bliley Act ("GLBA") requirements that have long imposed privacy and security requirements on financial institutions with respect to customer information. The following provides an overview of these state SSN protection policy requirements. Because the scope and underlying requirements of each state law differs, organizations should evaluate their potential obligations under each law separately.

Scope

The scope of each of these six state laws differs in terms of the entities subject to their respective requirements. For example, the Connecticut[8] and Michigan laws apply to any person who collects SSNs in the course of business. Similarly, the New York[9] law applies to any person that has possession of SSNs, but only to the extent that those SSNs are maintained for the conduct of business or trade.

The scope of the New Mexico and Texas laws, however, are narrower. For example, the New Mexico law applies only to a company that acquires or uses SSNs relating to "consumers." In New Mexico, the term "consumer" is defined as an individual who is a resident of New Mexico and who purchases, leases, or

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=da627d01-2b49-4239-9852-26274f107e74

otherwise contracts for products, goods, or services within New Mexico that are primarily used for personal, family, or household purposes. The Texas law applies to any person who requires that an individual disclose his or her SSN in order to obtain goods or services from, or enter into a business transaction with, the person. Based on the focus in these two laws on "consumers," it is not clear if either the New Mexico or Texas law applies to employees or to vendors.

The Massachusetts regulation applies to organizations that "own, license, store or maintain personal information," including SSNs, that relate to Massachusetts residents. Thus, read literally, a store in Kansas that accepts a credit card of an individual who resides in Massachusetts could be obligated to comply with the Massachusetts regulation, even if it has no other nexus to Massachusetts. It is also important to note that the Massachusetts law is much broader, as it applies to personal data other than just SSNs and has many other obligations contained in the regulations.[10]

SSN Protection Policy Safeguards

If a business is subject to any or each of these state laws, the business must first implement and maintain internal policies and procedures to protect SSNs. Specifically, a business must implement and maintain policies and procedures (its "SSN protection policy") that:

- protect the confidentiality and security of SSNs;
- prohibit the unlawful disclosure of SSNs;
- limit access to SSNs, including limiting access to SSNs to those employees who need such access to perform their job-related duties;
- document when employees can keep, access, and transport SSNs outside of business premises;
- provide for the proper disposal of SSNs; and
- provide penalties for violations of the SSN protection policy.

Moreover, a business must describe, in its SSN protection policy, how the business collects SSNs and how and when the business uses SSNs.

Disclosure Requirements

Connecticut, Michigan, and Texas laws require that a business disclose its SSN protection policy either to the general public or internally to its employees. For example, under the Michigan law, a business must publish its SSN protection policy in an employee handbook, procedures manual, or similar document that is available electronically. The Massachusetts law does not contain an explicit obligation to include a policy in an employee handbook or similar document; however, it requires the development of policies "for employees" and requires that an organization impose disciplinary measures for violations of its "comprehensive information security program rules." Thus, there is an implied obligation to make employees aware of the policy and rules.

The Connecticut and Texas laws, however, require broader, "public-facing" disclosures. For example, in order to comply with the Connecticut law, a business must publish or publicly display its SSN protection policy. In this regard, the Connecticut law clarifies that a business may post its SSN protection policy on its Internet web page. The Texas law imposes a more ambiguouspublic disclosure requirement. Specifically, if a business requires an individual to disclose his or her SSN in order to obtain goods or services from, or enter into a business transaction with, the business, it must make its SSN protection policy "available to the individual." Unlike the Connecticut law, the Texas law does not clarify whether publicly displaying an SSN protection policy, on the Internet for example, would meet this disclosure requirement. Moreover, under the Texas law, a public-facing SSN protection policy must address not only SSNs, but also "personal information."[11]

GLBA Exceptions

It is important to note that the Texas and Michigan laws provide GLBA exceptions. For example, the Texas law provides that the SSN protection policy requirement does not apply to "a person who is required to maintain *and* disseminate a [GLBA] privacy policy" (emphasis added). The scope of the Michigan exception, however, is less clear. Specifically, the Michigan law provides that the SSN protection policy requirement does not apply to "a person who possesses [SSNs] in the ordinary course of business and in compliance with" the GLBA.

The Connecticut, Massachusetts, New Mexico, and New York laws, however, do not include an explicit GLBA exception.

Practical Implications

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=da627d01-2b49-4239-9852-26274f107e74

These state SSN protection policy requirements highlight the importance of maintaining up-to-date privacy policies that comply with the evolving requirements under applicable state laws. To get started, an organization should consider taking the following steps:

- determine if you collect or maintain SSNs;
- review your policies and procedures that are employee-facing to determine if you have sufficient policies to meet the obligations under the various state laws;
- update your policies and procedures as needed;
- train employees on the new policies and procedures; and
- audit your employees to ensure that they are complying with your policies and procedures.

As a practical matter, the requirement to disclose an SSN protection policy imposes an additional burden on any business that is required to comply with these laws. Moreover, in light of the many state Unfair and Deceptive Acts and Practices Acts throughout the country, a business must ensure that it verifies the accuracy of, and complies with, any representations that it makes as part of its publicly disclosed SSN protection policy. Equally important, a business must ensure that its personnel substantially comply with its published SSN protection policy.

Footnotes

[1] *See, e.g.*, Cal. Civ. Code § 1798.84.
[2] Ct. H.B. 5658.
[3] 201 Mass. Code Regs. §§ 17.01 – 17.04.
[4] Mich. Comp. Laws § 445.84.
[5] N.M. Stat. §§ 57-12B-2 – 57-12B-3.
[6] N.Y. Gen. Bus. Law § 3990dd(4).
[7] Tex. Bus. & Com. Code § 35.581 (effective through March 31, 2009); Tex. Bus. & Com. Code § 501.051 – 501.053 (effective April 1, 2009).
[8] For more information about Connecticut's Act, see "New Connecticut Privacy Law Imposes Up to $500,000 in Civil Penalties for Misuse of Personal Information", Morrison & Foerster Legal Update (June 19, 2008), available at http://www.mofo.com/news/updates/bulletins/14042.html.
[9]For more information on the New York law, see "New York Limits Use and Disclosure Employee's Personal Identifying Information," Morrison & Foerster Legal Update (December 3, 2008).
[10] For additional information on the Massachusetts regulations, see "New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data Security Programs", Morrison & Foerster Legal Update (Sept. 23, 2008) and "Massachusetts Delays Effective Date of New Security Regulation", Morrison & Foerster Legal Update (Nov. 14, 2008) .
[11] The Texas law does not define the term "personal information."

© 1996-2008 Morrison & Foerster LLP. All rights reserved.