

# Preventing Identity Theft and Other Harm Through Increased Controls on Social Security Numbers: A Review of Select State Laws

JACQUELINE KLOSEK, AGNES BUNDY SCANLAN, AND RACHEL SAMUELS

*In the current climate, where data security breaches seem to occur on a daily basis and identity theft is rampant, the widespread use of Social Security numbers, and their availability to the public, is becoming increasingly regulated by the states. This article discusses the trends in state laws pertaining to Social Security numbers, and provides practical risk management strategies companies can use to protect the personal information in their possession.*

The Social Security number (“SSN”) is widely used by both public and private sector entities. Originally, SSNs were created to aid with benefits and retirement.<sup>1</sup> Today, SSNs are issued to almost every United States citizen and are even available to noncitizens in some cases.<sup>2</sup> SSNs are collected and used by a wide range of public and private organizations and entities, including one’s employer for benefit and payroll purposes,<sup>3</sup> banks and other financial institutions who verify identity and check credit using SSNs,<sup>4</sup> courts,<sup>5</sup> tax agencies,<sup>6</sup> and health care insur-

---

Jacqueline Klosek is senior counsel, Rachel A. Samuels is an associate, and Agnes Bundy Scanlan is counsel with the law firm of Goodwin Procter LLP. They can be reached at [jklosek@goodwinprocter.com](mailto:jklosek@goodwinprocter.com), [rsamuels@goodwinprocter.com](mailto:rsamuels@goodwinprocter.com), and [abundyscanlan@goodwinprocter.com](mailto:abundyscanlan@goodwinprocter.com), respectively.

ance companies when a person, or their employer, enrolls them in a plan.<sup>7</sup> Many state and local governments make the SSNs of certain individuals available in public records.<sup>8</sup>

In the current climate, where data security breaches seem to occur on a daily basis and identity theft is rampant, the widespread use of SSNs, and their availability to the public, is an issue since, according to the Government Accountability Office (“GAO”), “these numbers, along with a name and birth date, are the three pieces of information most often sought by identity thieves.”<sup>9</sup> To date, despite a number of proposals over the years, the federal government has not passed a comprehensive, uniform law to protect SSNs. A number of states, however, have enacted their own laws to protect SSNs in various ways. However, this raises problems for some entities, especially companies engaging in any form of interstate commerce, since the laws passed by these states are not uniform and contain varying provisions and requirements.

Public interest in limiting the use of SSNs was furthered on January 6, 2009 when Senator Dianne Feinstein (D-CA) introduced The Protecting the Privacy of Social Security Numbers Act (S.141). S.141 was cosponsored by Senators Gregg and Snowe and would “prohibit federal, state and local governments from displaying Social Security numbers on public records posted on the Internet or from printing them on government checks; prevent inmates from employment that would give them access to Social Security numbers of other individuals; and, provide limits on when businesses can ask customers for their Social Security numbers.”

In this article, we examine current trends in state laws that regulate the use of SSNs, with a particular emphasis on laws impacting the use of SSNs in the private sector.

## **TRENDS IN STATE LAWS THAT LIMIT COMPANIES’ USE OF SSNS**

Many states have enacted laws that limit how SSNs can be maintained and used by both public and private entities. While these laws vary by state, there are some features that many of the laws share and some new trends in state privacy laws.

## Notification of Unauthorized Access to or Acquisition of Personal Data

One of the most widespread measures for protecting SSNs at the state level has been through breach notification laws. Approximately 44 states, the District of Columbia and Puerto Rico have adopted security breach notification laws that require that a person be notified when their personal information, including their SSN, has been compromised.<sup>10</sup> California, one of the first states to enact a security breach notification law, adopted a statute in 2002 that requires that people be notified when their personal information was, or is reasonably believed to have been, acquired by an unauthorized person.<sup>11</sup>

The New York statute, like the breach notification laws of many other states, closely follows the California model.<sup>12</sup> Specifically, the New York statute requires that, “[a]ny person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.”<sup>13</sup> Additionally, the New York statute has a provision that requires any person or business that maintains computerized data *that it does not own* to notify the owner or licensee of the breach.<sup>14</sup> This is a very important provision, as it enables companies to know of breaches experienced by their vendors and service providers, irrespective of the terms of the underlying vendor contract. The New York breach notification statute applies to any person or business that conducts business in New York. It does not apply to entities not doing business in the state but who collect SSNs of state residents.<sup>15</sup>

Security breach notification laws were one of the first steps that many states took toward protecting SSNs and preventing identity theft. However, these laws only apply and help to make people aware when their SSN has been or could have compromised. Security breach notification laws do not intend to prevent the person’s SSN from being compromised in the first place. As such, more recent trends have focused on measures that aim to help prevent SSNs from being compromised in the first place.

## Restrictions on Display and Use of SSNs

Connecticut has implemented a privacy law that restricts the display and use of SSNs.<sup>16</sup> One provision of the Connecticut law provides that no person may “[p]ublicly post or publicly display in any manner an individual’s Social Security number,”<sup>17</sup> with “publicly post” and “publicly display” meaning, “to intentionally communicate or otherwise make available to the general public.”<sup>18</sup> The Connecticut law also has prohibitions against placing an individual’s SSN on an identification card, requiring people to send their SSNs on the Internet without proper precautions, and requiring a person to use their SSN to access web sites without other security measures.<sup>19</sup> The law’s implications are limited through the definition of “person,” which exempts the state, any subdivision thereof, and any state agencies.<sup>20</sup> While this law is helpful in prohibiting the use of SSNs on identification cards and Internet web sites, the limited applicability to private entities leaves gaps in the protection afforded under the law.

Arizona has also enacted a law to protect SSNs by placing restrictions on their display and use.<sup>21</sup> The Arizona law is almost identical to the Connecticut law, except that it adds a provision restricting the use of SSNs on items that are mailed to a resident.<sup>22</sup> The Arizona statute, unlike the Connecticut statute, provides some restrictions on use of SSNs by the state and subdivisions of the state. Under the statute, SSNs cannot be used by the state or any subdivision of the state on identifications cards that they issue.<sup>23</sup> However, the Arizona statute continues to allow agencies of the state and subdivision of the state to disseminate or use the last four numbers of a person’s SSN.<sup>24</sup> The Arizona statute applies to any entity that obtains or maintains the SSNs of residents of the state.<sup>25</sup>

Minnesota’s statute on the use and display of SSNs is practically identical to the Arizona statute.<sup>26</sup> The Minnesota statute applies to “a person or entity, not including a government entity.”<sup>27</sup> Therefore, the Minnesota statute applies only to private entities. The statute contains the provisions of the Connecticut and Arizona statutes pertaining to public posting and use, identification cards, the internet, and mailings.<sup>28</sup> In addition, the Minnesota statute includes provisions that prohibit “assign[ing] or us[ing] a number as the primary account identifier that is identical to or incorporates an individual’s complete Social Security number, except in conjunc-

tion with an employee or member retirement or benefit plan or human resource or payroll administration,<sup>29</sup> and which prohibit selling “Social Security numbers obtained from individuals in the course of business.”<sup>30</sup>

Virginia has a similar statute on the restrictions of SSNs. The Virginia statute also prohibits intentionally disclosing a person’s SSN, printing an individual’s SSN on a card required for obtaining products or services, requiring an SSN to access a web site unless other security and authorization measures are used, and having an individual’s SSN visible in any mailing, whether on the outside or inside of the mailing.<sup>31</sup> Laws such as these that operate as restrictions on the display and use of SSNs may help to limit the widespread accessibility of SSNs, thus helping to prevent identity theft.

## Privacy Policy Requirements

In addition to the statute covering use and display of SSNs, Connecticut has a Public Act that pertains to privacy policies applicable to SSNs. Under the act, Public Act No. 08-167, which became effective October 1, 2008, any person who collects SSNs in the course of business must create and publicize a privacy policy.<sup>32</sup> The act specifies that the policy must “(1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers.”<sup>33</sup> The act does not apply to any agency or subdivision of the state.<sup>34</sup>

Michigan has a statute that requires a person who obtains one or more SSNs to have a privacy policy that applies to such SSNs.<sup>35</sup> The policy must ensure confidentiality of SSNs, prohibit unlawful disclosure of SSNs, limit who has access to SSNs, describe how to dispose of documents containing SSNs, and establish penalties for violations of the policy.<sup>36</sup> Certain laws, such as the Michigan statute, make an exception for persons or entities that comply with the requirements of the federal Gramm-Leach-Bliley Act, 15 U.S.C. 6801 to 6809, or other federal statutes.<sup>37</sup> The Michigan statute provides an exemption for “a person who possesses social security numbers in the ordinary course of business and in compliance with the fair credit reporting act, 15 USC 1681 to 1681v, or subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to

6809.”<sup>38</sup> Other states’ laws do not contain such exemptions. Without such an exemption, companies in those states that are in compliance with Gramm-Leach-Bliley and other statutes may still need to alter their policies and procedures to be in compliance with state laws.

Several states have adopted laws that require the state, and its subdivisions and agencies, to place a privacy policy on their web sites where personal information, including SSNs, is collected through such site. One state with such a law is Montana. The Montana statute requires that if the government operator of a web site collects personally identifiable information, which includes SSNs, the operator of the web site must ensure that the web site identifies who operates the web site, provides contact information for the operator of the web site, and “generally describes the operator’s information practices, including policies to protect the privacy of the user and the steps taken to protect the security of the collected information.”<sup>39</sup>

### **Specific Information Security Requirement**

Another emerging trend in state privacy laws is seen in statutes that require specific information security requirements and encryption of personal data, including SSNs. A Nevada statute that became effective October 1, 2008, requires that “[a] business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”<sup>40</sup> The Nevada statute appears to apply only to businesses located within the state, and not to any business that is doing business in the state.

The Massachusetts Office of Consumer Affairs and Business Regulation recently enacted regulations pertaining to identity theft and data security.<sup>41</sup> The regulations have broad coverage since they apply to all entities that “own[], license[], store[] or maintain[] personal information about a resident of the Commonwealth,”<sup>42</sup> and not only those entities that are located or operate in the state. Additionally, the definition of “person” in the regulations is broad, including “a natural person, corporation, association, partnership or other legal entity, other than an agency, execu-

tive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.”<sup>43</sup> The regulations require that “[e]very person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.”<sup>44</sup> The Massachusetts regulations also have provisions governing the encryption of data, including SSNs. The regulations require that all transmitted records and files that contain personal information be encrypted when transmitted wirelessly or over a public network.<sup>45</sup> The regulations also require encryption of all personal information that is “stored on laptops or other portable devices.”<sup>46</sup> The Massachusetts statute is one of the broadest encryption laws to have been passed thus far. The new Massachusetts privacy regulations do not contain an exemption for other compliance, such as compliance with the federal Gramm-Leach-Bliley Act, 15 U.S.C. 6801 to 6809, or other federal statutes.<sup>47</sup> The regulations require that all persons must comply with the stringent requirements of the regulations. Since the Massachusetts regulations have no exemption for persons who comply with Gramm-Leach-Bliley, even companies that are already in compliance may have to rework their privacy policies to comply with the Massachusetts regulations.

The State of Washington has a proposed bill that would require the encryption of data.<sup>48</sup> The Washington proposal would add a section that reads “[a]ny person or business that, in the regular course of business and in connection with an access device, collects or stores personal information must comply with payment card industry data security standards established by the PCI security standards council.”<sup>49</sup>

Further, a bill in the Michigan Senate would require data encryption.<sup>50</sup> The Michigan law would add a subsection to Michigan Compiled Laws §445.71.<sup>51</sup> The subsection would state, “[i]f the person collects personal identifying information in the regular course of business and stores that information in a computerized data base, failing or neglecting to store that information in the database in an encrypted form, in conformity with current industry-standard encryption methods and capabilities.”<sup>52</sup>

The Massachusetts regulations are by far the most stringent of these

new measures but they are not likely to be the last. States are continuing to seek out the most effective means for protecting SSNs and preventing identity theft.

## **RISK MANAGEMENT STRATEGIES**

A large, growing, and diverse group of laws exist that protect SSNs at the state level. These laws have diverse applications, with some of the laws applying only to companies doing business in a state, some applying to companies collecting SSNs or other personal information from residents of the state, and some applying only to companies that are located in the state. It is important that companies remain aware of the rapidly evolving legal and regulatory environment.

Nonetheless, certain principles of good practice apply to all companies. Companies should limit the collection of all personal information, especially SSNs, to what is needed for particular purposes. It is important for companies to develop and implement security policies to protect privacy and the personal information that they collect or maintain. Companies need to implement employee training on the policies and guidelines that they develop for protecting personal information and SSNs. Furthermore, companies ought to conduct due diligence on vendors and other third parties as well as use stringent contract provisions relating to privacy with vendors and other third parties. Taking these steps will help companies protect personal information, including SSNs, and is a first step toward compliance. Companies do, however, need to check the applicable state laws and ensure compliance. Furthermore, as this is a rapidly emerging area, continuous monitoring of developing legislative framework is warranted.

## **NOTES**

<sup>1</sup> Barbara D. Bovbjerg, Dir. Educ., Workforce, and Income Sec. Issues, Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain, Testimony before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, N.Y. State Assembly (Sept. 15, 2005), in GAO-05-1016T [hereinafter *GAO SSN Publication*] at 3.

<sup>2</sup> *Id.* According to the GAO, “[t]oday, SSA issues SSNs to most U.S. citizens, but they are also available to noncitizens lawfully admitted to the United States with permission to work. Lawfully admitted noncitizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires that they have a SSN to obtain a particular welfare benefit or service.” *Id.*

<sup>3</sup> *Id.* at 6.

<sup>4</sup> *See Id.* at 1, 2, 9.

<sup>5</sup> *See Id.* at 7.

<sup>6</sup> *See Id.* at 6.

<sup>7</sup> *Id.* at 9.

<sup>8</sup> *Id.* at introductory page.

<sup>9</sup> *Id.* at 3.

<sup>10</sup> Miriam Wugmeister and Nathan D. Taylor, United States: Six States Now Require Social Security Number Protection Policies, Dec. 10, 2008, available at <http://www.mondaq.com/article.asp?articleid=71322>.

<sup>11</sup> CAL. CIV. CODE § 1798.29(a) (2002); *See GAO SSN Publication, supra* note 1, at 14. The California law states that “Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been required by an unauthorized person.” CAL. CIV. CODE § 1798.29(a) (2002).

<sup>12</sup> N.Y. GEN. BUS. LAW. § 899-aa.

<sup>13</sup> N.Y. GEN. BUS. LAW. § 899-aa(2).

<sup>14</sup> N.Y. GEN. BUS. LAW. § 899-aa(3).

<sup>15</sup> N.Y. GEN. BUS. LAW. § 899-aa(2).

<sup>16</sup> *See* CONN. GEN. STAT. § 42-470.

<sup>17</sup> CONN. GEN. STAT. § 42-470(b)(1).

<sup>18</sup> *Id.*

<sup>19</sup> CONN. GEN. STAT. § 42-470(b)(2)-(4).

<sup>20</sup> CONN. GEN. STAT. § 42-470(a).

<sup>21</sup> ARIZ. REV. STAT. § 44-1373.

<sup>22</sup> ARIZ. REV. STAT. § 44-1373(A).

<sup>23</sup> ARIZ. REV. STAT. § 44-1373(D).

<sup>24</sup> ARIZ. REV. STAT. § 44-1373(E).

<sup>25</sup> ARIZ. REV. STAT. § 44-1373. Section K of the statute provides that in this

section, “individual” means a resident of the state. ARIZ. REV. STAT. § 44-1373(K).

<sup>26</sup> MINN. STAT. § 325E-59(1)(a) (2008).

<sup>27</sup> *Id.*

<sup>28</sup> MINN. STAT. § 325E-59(1)(a)(1)-(5) (2008).

<sup>29</sup> MINN. STAT. § 325E-59(1)(a)(6) (2008).

<sup>30</sup> MINN. STAT. § 325E-59(1)(a)(7) (2008).

<sup>31</sup> VA. CODE ANN. § 59.1-443.2 (2008).

<sup>32</sup> 2008 Conn. Acts 08-167(1)(b).

<sup>33</sup> *Id.*

<sup>34</sup> 2008 Conn. Acts 08-167(1)(f).

<sup>35</sup> MICH. COMP. LAWS § 445.84 (2004).

<sup>36</sup> *Id.*

<sup>37</sup> MICH. COMP. LAWS § 445.84(3) (2004). The Gramm-Leach-Bliley Act provides privacy guidelines and requirements for financial institutions. See Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 to 6809 (1999).

<sup>38</sup> *Id.*

<sup>39</sup> MONT. CODE ANN. § 2-17-552 (2007).

<sup>40</sup> NEV. REV. STAT. § 597.970(1).

<sup>41</sup> 201 MASS. CODE REGS. 17.00 *et seq.* These regulations implement the provisions of chapter 93H of the General Laws of Massachusetts.

<sup>42</sup> *Id.*

<sup>43</sup> 201 MASS. CODE REGS. 17.02.

<sup>44</sup> 201 MASS. CODE REGS. 17.03.

<sup>45</sup> 201 MASS. CODE REGS. 17.04(3).

<sup>46</sup> 201 MASS. CODE REGS. 17.04(5).

<sup>47</sup> *See* 201 MASS. CODE REGS. 17.00 *et seq.*

<sup>48</sup> S.B. 6425, 60th Leg., 2008 Reg. Sess. (Wash. 2008).

<sup>49</sup> *Id.* at Sec. 4.

<sup>50</sup> S.B. 1022, 94th Leg., Reg. Sess. (Mich. 2008).

<sup>51</sup> *Id.*

<sup>52</sup> *Id.* The new section would have been Subsection (e) to Michigan Compiled Laws § 445.71(1).