Does California Privacy Law SB 168 Apply To Your Organization?

Rebecca Herold, CISM, CISSP, CISA, FLMI

(Note: Originally published in the September 2002 CSI Alert)

In the early 1990's I became very concerned about how social security numbers (SSNs) were becoming so widely used as account numbers…for insurance policies, bank accounts, and a number of other services and products. When I expressed my concern to my employer at the time, and discussed with corporate legal counsel, I was told that there was no law against using SSNs as account numbers, and that there was way too much programming code that would have to be changed to use something different, that the expense would be prohibitive considering there was no compelling reason (e.g., law) to make such a change, and there were other more pressing issues to address besides the remote possibility of having someone gain inappropriate access to a customer's SSN and nab their identity. So, thank you very much for bringing up the issue, now run along and work on something else please. Hmm…sure, okay.

In the years since this first encounter with trying to address the issue of SSN use, the number of organizations that created new systems and procedures utilizing SSNs as account numbers and authentication information continued to grow dramatically. During this same time, the number of identity theft occurrences continued to grow, as did the public's awareness of the relationship between the access to SSNs and the ease with which fraud and identity theft could occur by using SSNs. States and politicians started to take notice.

On October 11, 2001, California Bill number SB 168 was signed into law and certain requirements within the law became effective on July 1, 2002, with other directives going into effect on January 1, 2003. The goal of the act is to reduce the huge number of identity theft incidents in California and to try and ensure the privacy of certain types of information about California residents, including SSNs. This was followed by Civil Code Section 1798.85 which expanded upon the specific activities for what could and could not be done with California residents' SSNs. So, what does this have to do with you if your organization is not in California? Well, if your organization has customers who are California residents, and your organization uses the SSN as an account number, or as an authentication method for customers to gain access to accounts, your organization could be liable for violating one of the California codes. Several states place some restrictions on the use of SSNs, but California is the first state in the U.S. to enact law specifically addressing such a wide range of SSNs restrictions. Other states are taking notice and considering following suit.

What are the limitations on SSN use required by SB 168 and supported by the requirements in Civil Code Section 1798.85? Because the goal of the bill is to reduce identity theft, many other requirements other than SSN limitations are included in the bill. However, with respect specifically to SSNs, as of July 1, 2002 organizations:

- Cannot post or display SSNs publicly
- Cannot print SSNs on identification badges or cards required to access services or products

- Cannot require SSNs to be transmitted over the Internet unless the connection is "secure" or the SSN encrypted
- Cannot require individuals to use SSNs to access a web site without additionally requiring a password or other authentication device
- Cannot print SSNs on documents mailed to individuals
- Cannot require SSNs as a condition to gain access to products or services
- Must allow individuals to make a written request to prohibit the use of his/her SSN, make the change within 30 days, and not charge the individuals for implementing the request

The provisions of this law do not prevent the collection, use, printing or retention of SSNs as required by state or federal law, or the use of SSNs for internal verification or administrative purposes (such as on an application form). All businesses must comply with all requirements for every ***new customer*** since July 1, 2002. For existing customers, businesses can continue their former practices unless otherwise requested. However, they must make a yearly disclosure to such existing customers notifying them of their right to request their SSN to not be used in the ways indicated earlier. Health care businesses (for example, a health care service plan, a health care provider, an insurer or a pharmacy benefits manager or contractor) are exempted from this deadline, but must phase in the new law from January 1, 2003 to July 1, 2005, depending upon their situation.

So, if your organization has customers who are California residents, then check with your legal counsel to determine specifically how this law applies to you. When making such a determination, consider:

- Do you use SSN as an identifier?
- Do you use SSN as an account number?
- Do you print SSNs on mailings to customers?
- Do you print SSNs on identification or service cards?
- Do you provide access to customer listings (for example, on a web site or in printed publications) that include their SSNs?
- Do you require customers to provide an SSN to gain access to their account information over the phone or on a web site?
- Do you have a procedure in place to replace an existing customer's account number that is an SSN with something else if they make this request?
- Can you replace existing customer account numbers that are SSNs with something else within 30 days of such a request?

Even if you don't have any customers who are California residents, keep in mind that it is likely that soon the winds of time will blow similar laws your way from other states in which you DO have customers. And, even if you do not do business where the use of SSN is prohibited, don't you think it's a good idea to use some other type of numbering scheme as an account number or authentication device? What…I should run along and worry about something else? Hmm…sure, okay.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at

rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.

