LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 29, Number 5 • August 2014

Collecting Social Security Numbers

By Nicole Pszczolkowski and L. Elise Dieterich

In the first six months of 2014, at least 96 significant data breaches were reported, compromising more than 2.2 million records, according to the Privacy Rights Clearinghouse. Of these breaches, at least 46 involved records that may have contained Social Security Numbers (SSNs). What the affected businesses may not know is that their mere collection of SSNs may have put them in violation of state laws, in addition to the liability they may now face for having failed to protect the SSN information.

Despite their limited original purpose, SSNs have become *de facto* national identifiers, frequently used as an authenticator in both the public and private sectors. In fact, no other form of personal identification plays a more significant role in linking together records that contain an individual's sensitive and confidential information. Ironically, the widespread use of SSNs as both an identifier and an authenticator is precisely what makes collecting and using the numbers so risky.

Not surprisingly, the fact that SSNs serve as the keys to unlock a host of personal, medical, and financial information about individuals makes them highly desirable to criminals, such as identity thieves. And, thanks to never-ending technological advancements, SSNs are increasingly being transmitted and stored electronically, vastly expanding nefarious actors' ability to wrongfully obtain them. Given this climate, numerous state and federal laws have been enacted to limit the collection, use and disclosure of SSNs.

As a result, the presence of customer, patient, or employee SSNs in your business records, whether collected intentionally for a specific business purpose or inadvertently as part of an unrelated request, adds yet another layer of potential data-related liability. Although most businesses understand that they should limit the disclosure of SSNs consistent with state and federal laws, they may be unaware of the state laws placing restrictions on businesses' ability to request, collect, or store SSNs in the first place.

This article suggests a framework for ensuring compliance with the majority (albeit not all) of the applicable state laws and avoiding the financial, legal and reputational damage that can occur when SSNs are improperly collected, used or disclosed.

An Overview of SSN Restrictions

While federal laws typically focus on limiting the use and disclosure of SSNs in specific circumstances, such as in connection with medical information (HIPAA), student information (FERPA), or credit information (FCRA), more than 40 states have enacted laws restricting the collection and/or use of SSNs.

Several of these state laws limit to varying degrees the purposes for which SSNs can be collected. Alaska, for example, categorically prohibits businesses from collecting SSNs unless for fraud prevention, medical treatment, or to perform a background check on an individual. The majority of states, however, still allow for the collection of SSNs under a broader set of circumstances, including in connection with an individual's employment and employment benefits, for law enforcement or other government purposes, and for verification of an individual's age or identity.

At least six states require businesses that collect SSNs to have some form of written privacy policy in place. Texas, for example, prohibits requiring an individual to provide an SSN, unless the requesting entity has in place a privacy policy, a copy of which is provided to the individual, that addresses: 1) how personal information is collected; 2) how and when the personal information is used; 3) how the personal information is protected; 4) who has access to the personal information; and 5) the method of disposal of the personal information.

Massachusetts requires businesses that collect SSNs (as well as other personally identifiable information) of any Massachusetts resi-

Nicole Pszczolkowski is an associate in Kutak Rock LLP's Washington, D.C., office. L. **Elise Dieterich** is a partner and the leader of Kutak Rock's privacy and data security practice in D.C., and a member of this newsletter's Board of Editors.

dent (regardless of where the business is located) to have in place a comprehensive written information security program (WISP) that satisfies stringent and detailed administrative, technical and physical data security requirements. For example, the Massachusetts law and accompanying regulations require WISPs for organizations that electronically store or transmit personal information to establish a computer security system that at a minimum includes: 1) encryption of all sensitive information; 2) secure user authentication and access control measures; 3) unauthorized use monitoring; 4) up-to-date firewall and malware protection; and 5) operating system security patches.

Additionally, all businesses' WISPs must include: 1) assessment on an ongoing basis of reasonably foreseeable internal and external risks to records containing personal information, and adoption of steps to mitigate those risks; 2) designation of one or more employees to maintain and monitor the WISP; 3) development of security policies for employees and the imposition of disciplinary measures for violations; 4) documentation of responsive actions taken in connection with breaches; and 5) a requirement that third-party service provider contracts mandate implementation and maintenance of the security measures set forth in the business's security plan.

Once SSNs are collected, both federal and state laws impose restrictions on companies' ability to use SSNs. The majority of state laws are similar to California's (California is often considered to be a bellwether state in the privacy arena), which permits collection of SSNs, but prohibits: 1) public posting or public display of SSNs; 2) printing or electronically embedding an individual's SSN on a card required to access products or services; 3) requiring an individual to transmit an SSN over the Internet, unless encrypted or over a secure connection; or 4) printing an SSN on materials mailed to an individual.

Should Your Business Collect SSNs?

In view of these state and federal restrictions on the collection, storage, and use of SSNs, and the risk a business incurs when it has SSNs in its possession, it is strongly recommended that businesses collect and use SSNs only on an as-needed basis (*i.e.*, only when required to do so by federal or state law, or when no other form of identification will suffice). At a minimum, businesses should audit their data collection practices to determine in what context, and for what purposes, SSNs are being collected.

In many instances, SSNs are inadvertently collected when customers, patients, or employees are asked to submit necessary information, such as educational, medical, or veterans' records, that happens also to include the individual's SSN. If this is occurring, the business should make a conscious determination about whether the collection of the SSN is necessary, or whether that data element could be redacted from the form on which it appears.

If SSNs are being collected to provide a unique personal identifier for the customer, patient, or employee, businesses should consider developing their own internal identifier as a substitute for the SSN. Ideally, if your business has no compelling reason to have SSNs, there shouldn't be any SSNs in your electronic or paper files. Data you do not have cannot be breached!

If SSNs Are Necessary, How Should They Be Handled?

If the collection of SSNs is essential to your business, we recommend (and, in many cases, the law requires) the following "best practices" for handling such information:

Eliminate Public Display and Unencrypted Transmission of SSNs

- Never publicly post or display an individual's SSN.
- Never print an individual's SSN on any personal identification card or badge.
- Never print an individual's SSN on any piece of mail that is being sent to the individual.
- Never require an individual's SSN to be transmitted or used over the Internet unless the connection is secure and the SSN is encrypted.
- When possible, redact an individual's SSN when keeping a document on file or encrypt the SSN when storing electronically.
- Never require an individual's SSN to be used as a login or password on any Internet site.
- Note that even the last four digits of an SSN can be enough to enable identity theft — omit any reference to SSNs whenever possible.

Control Access to SSNs

- Limit access to records containing SSNs to only those who need to see the numbers for the performance of their duties.
- Never store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Avoid sharing SSNs with other companies or organizations, and use written agreements to protect confidentiality if sharing is necessary.

Protect SSNs with Security Safeguards

- Develop — and enforce — a written security plan for record systems that contain SSNs.
- Encrypt SSNs in electronic records and store hard-copy records and removable media

(such as disks, tapes, or USB drives) in locked cabinets.
- Provide for secure destruction of all documents and electronic files containing SSNs when no longer needed.

Ensure Accountability for Protecting Safeguards

- Provide employees with training and written materials addressing their responsibilities in handling SSNs.
- Conduct risk assessments and regular audits of record systems containing SSNs.
- Designate someone at your company to be responsible for ensuring compliance with policies and procedures for protecting SSNs.
- Implement specific privacy policies to protect SSNs and make such policies available to your customers, patients, or employees whose SSNs you collect.

Additionally, it is recommended that you inform individuals from whom you collect SSNs of the purpose of the collection, the intended use, whether the law requires the SSN to be provided or not, and the consequences of not providing the number.

While following these guidelines will enable compliance with the majority of the current federal and state laws addressing the collection, use, and disclosure of SSNs, such actions may not ensure compliance with every applicable law, particularly in those states, such as Alaska, Texas, and Massachusetts, with the most stringent requirements. Moreover, each new high-profile data breach prompts legislators to reexamine businesses' data collection practices, and new privacy laws are enacted each year. To the extent your business has a need to collect SSN numbers, or is at risk for inadvertently collecting such information, consultation with privacy counsel and assessment of the specific laws applicable to the jurisdictions in which you operate should be undertaken on a regular basis.

Other Risky Data Elements

SSNs are not the only data element that can cause unexpected risks for businesses — others include ZIP codes, driver's license numbers, and cell phone numbers. For example, in 2011, the California Supreme Court in *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524 (2011), held that ZIP codes are "personal identification information" subject to protection under the state's Song-Beverly Credit Card Act of 1971. Similarly, two years later, the Massachusetts high court deemed ZIP codes "personal identifying information" in *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492 (2013).

Another key judicial decision involving the collection and use of ZIP codes is expected soon in a case that was pending in the U.S. District Court in Massachusetts at press time. In *Alberts v. Payless Shoesource, Inc.* (D. Mass. Case No. 1:13-cv-12262, filed Sept. 12, 2013), Payless Shoesource, Inc. moved to dismiss a putative class action on the basis that its customers voluntarily provided their ZIP codes when asked at checkout, and the ZIP code information is stored in a database separate and distinct from the credit card transaction forms — thus, Payless argues, Massachusetts' prohibition on requiring customers to provide their ZIP codes in order to complete a credit card transaction does not apply.

Additionally, the use of cell phone numbers collected from customers for "robocalls" has generated class action litigation — and major settlements — in a number of recent cases. Companies settling in the past year include giants such as Bank of America, JP Morgan Chase, and Papa Johns Pizza.

Also of particular interest to merchants are laws such as the one enacted in Texas, which imposes collection, use and disclosure limitations, as well as destruction requirements, on businesses that collect and use driver's license numbers. Continue to check back with *The Corporate Counselor* for future articles providing guidance on businesses's collection and use of these and other data elements.

Conclusion

Bottom line? In this era of hackers, big data, and ever more restrictive state and federal privacy laws, no data element that is connected to an individual is entirely benign. Data collection, while essential, has become inherently risky for businesses, and SSNs are just one example of why now, more than ever, businesses should be educating themselves about the privacy laws, and assessing their data collection, storage, and use practices.

KUTAK ROCK LLP®