Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

NEW YORK PENNSYLVANIA CALIFORNIA WASHINGTON, DC NEW JERSEY DELAWARE

Labor & Employment
ALERT

JULY
2008

CONNECTICUT ENACTS BOLD NEW DATA PRIVACY LAW

Starting October 1, 2008, businesses and individuals in Connecticut that collect Social Security numbers ["SSNs"] and any other "personal information" from employees, customers and others will have important new obligations in maintaining and disposing of that data. Agencies charged with enforcing these new obligations will be armed with the authority to seek extremely stiff civil fines – up to $500,000 – for an intentional failure to comply with the law's protective requirements. In signing H.B. 5658, which became Public Act No. 08-167, (the "Act") Connecticut's Governor Rell cited identity theft as the principal target, calling it "one of the most frightening non-violent crimes of the 21st Century," and one that "has become all too common." Governor Rell has a firm foundation for her statement: within the past year, the state's Department of Revenue Services disclosed that a laptop containing personally identifiable data on more than 106,000 taxpayers went missing from its custody.

The Obligations

The Act will require businesses, including their human resources or other employment functions, to protect personal information and SSNs during their possession and use of that data, and ultimately in disposing of it. The information must be protected regardless of whether it is maintained on paper or stored electronically. While the most vigorous measures are reserved for SSNs, all forms of personal information in the possession of a business or any other person will require protection, including during disposal of the data. The nature of the obligations will depend on whether the data is or includes SSNs or falls into a category of other personal information.

Privacy Protection Policies for SSNs. Any person who collects SSNs in the course of business in Connecticut will be required to prepare and post a *Privacy Protection Policy*. This policy must at a minimum accomplish three aims: (1) protect the confidentiality of SSNs; (2) prohibit unlawful disclosure of SSNs; and (3) limit access to SSNs. It is important to note that the Act does not stop at mere implementation of a policy; it requires that the policy be "publicly displayed." According to the Act, this "includes, but is not limited to, posting on an Internet web page." This suggests that to better ensure compliance, something further should be done to publish the policy, such as posting a physical copy at some logical location that is accessible to customers, employees and others whose SSNs are obtained.

Protection of "Personal Information." The Act protects more than SSNs. It also establishes a second category of protected information which it denominates *personal information*. This consists of "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a SSN, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number." However, it excludes specific publicly available information. The Act directs that "any person in possession of personal information of another person ... [must] … .safeguard the data, computer files and documents containing the information from misuse by third parties *and* destroy, erase or make unreadable the data, computer files and documents prior to disposal." (Emphasis added.)

(continued on page 2)

(continued from page 1)

Enforcement. The Act will be enforced by the state regulatory agency that licensed the business where applicable. Enforcement for others will be the responsibility of the state Department of Consumer Protection. The availability of penalties of up to $500,000, which can be assessed for intentional violations of the Act's requirements only, reflect the high level of concern that prompted the law's enactment.

Comments and Recommendations

Although the limitation of penalties to instances of intentional violation of the Act should be of some comfort, a serious data breach need not occur for there to be a violation – much less an intentional one. The civil penalty of up to $500,000 can be imposed not only for a willful failure to safeguard personal data, but also for intentional failures by businesses to properly dispose of such data or to create and/or post a written Privacy Protection Policy, and failure to follow the use restrictions on SSNs prescribed by the new law. The potential size of the penalties was dramatically increased from the original version of the Act, evidencing a "get tough" intent by the Legislature on those who might flout these measures. Whether this attitude will animate the enforcement agencies remains to be seen.

For employers, the Act adds still another layer of regulatory requirements. However, because a data breach presents a source of potentially serious liability to employees and customers alike, compliance is consistent with employers' long term interests. Therefore, employers should consider more than minimal compliance, adding some of the following to their data protection strategy:

- Inclusion of all personal data in their Privacy Protection Policy mandated for SSNs;
- Creation of mandatory procedures for destruction of personal information, including shredding of paper documents and destruction of data on hard drives. Simple erasure will not be adequate.
- Training of employees in recognizing, handling, maintaining and destruction of personal information, and for recognizing, reporting and otherwise handling a data security breach;
- Installation and use of encryption software;
- Promulgation and enforcement of strict rules limiting access to SSNs and personal information and prohibiting their removal and/or transfer to other locations;
- Creation of an integrated strategy with vendors for addressing common personal data protection issues.

Conclusion

While adequate time exists before the October 1 effective date, businesses having employees and/or customers in Connecticut should begin preparing to comply with the Act. As the Connecticut statute does not exist in a vacuum, this also is a good time to analyze how compliance can fit into a business's overall strategy for protecting SSNs and other personal data of employees and customers. At present, the absence of a comprehensive federal data protection scheme means that compliance standards differ from state to state; what satisfies regulators in one state may be insufficient in another. With state legislatures only recently beginning to regulate the data protection area, the complexity caused by a thicket of differing standards, using differing definitions and protecting different categories of data, will not become more easily navigable anytime soon. There is no better time to begin or update compliance efforts than the present. ◆

For further information, please contact:

Scott J. Wenner
(212) 973-8115
swenner@schnader.com