ASAP™
A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

JUNE 2008

New Connecticut legislation imposes privacy protection obligations upon employers, and threatens steep financial penalties for non-compliance. As of October 1, 2008, Connecticut employers must create, publish and maintain a policy protecting any retained Social Security numbers from disclosure and must take affirmative steps to safeguard a broad spectrum of private information.

East Coast Edition

A Littler Mendelson East Coast-specific Newsletter

Connecticut Becomes Only the Second State to Mandate an Employee Data Protection Policy

By Philip L. Gordon and Kate H. Bally

With the State of Connecticut reeling from a series of massive security breaches that have exposed the personal information of hundreds of thousands of state residents, Connecticut's Governor and General Assembly joined forces in mid-June to make Connecticut only the second state (after Michigan) to mandate that private employers publish a policy on the protection of employee Social Security numbers (SSNs). The new Connecticut law — entitled, "An Act Concerning the Confidentiality of Social Security Numbers" (the "Act"), and effective October 1, 2008 — also imposes on private employers a statutory duty to safeguard, and properly dispose of, personal information more broadly defined.

Employers Must Create and Post a Social Security Number Policy. The Act requires the creation of a "a privacy protection policy" by any entity that collects SSNs in the course of its business. The Act does not limit this requirement to the collection of SSNs from any particular category of individuals, such as customers, patients, or insureds. The Act, therefore, necessarily encompasses the collection of SSNs from employees. Consequently, the Act requires employers to promulgate a policy that, at a minimum, (1) protects the confidentiality of SSNs; (2) prohibits unlawful disclosure of SSNs; and (3) limits access to SSNs.

The Act requires the publication or public display of the privacy protection policy. It is unclear, however, how this requirement applies to employers as the Act's only example of "public display" is "posting on an Internet web site." An employer, presumably, can satisfy the publication requirement by publishing its privacy protection policy in an employee handbook or by posting the policy on the corporate intranet.

Confidentiality of Other Personal Information. Although the policy required by the Act need only address SSNs, the Act also imposes information security requirements with respect to "personal information," broadly defined. More specifically, employers must safeguard that information from misuse by third parties and must destroy it in a manner that renders the information irrecoverable, e.g., shredding paper documents and running a "cyberscrub" program before disposing of electronic storage media. These requirements apply to any "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, 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."

Enforcement by Agencies. For persons holding a license, registration or certification issued by agencies other than the Department of Consumer Protection, only the licensing agency will enforce the Act. For all other businesses, the Department of Consumer Protection will enforce the Act. While the Act does not

authorize a private right of action for violations, the Act's requirements arguably establish a standard of care that could be used to support a negligence lawsuit against an employer who fails to adequately safeguard personal information.

Fines Imposed, but Not for Unintentional Violations. Significantly, the Act specifically excludes unintentional violations from its purview. Intentional violations, however, can result in a civil penalty of $500 per violation, not to exceed $5,000 dollars per single event. Although the Act requires the depositing of any fine into a specific Privacy Protection Guaranty and Enforcement Account, the bill proposing the creation of such account did not pass into law. Such fines, therefore, likely will be deposited into the General Fund.

Recommendations. Although the Act mandates publication of a policy only regarding SSNs, Connecticut employers should consider implementing a broader employee data protection policy to encompass all categories of personal information that must now be safeguarded in accordance with the Act. Connecticut employers can facilitate drafting such a policy by evaluating how their organization uses, discloses, and safeguards personal information and to find ways to limit use, restrict disclosures, and enhance safeguards.

The results of this evaluation then can be used to formulate a policy that addresses the following topics, among others:

- Implementing administrative, physical and technical controls to restrict access to personal information to those with a need to know;
- Authorizing access to personal information only for employees who, through years of service, are known to be trustworthy or who have undergone a background check;
- Centralizing responsibility for disclosure of personal information with one senior-level manager or in one office to reduce the risk of unauthorized disclosures;
- Establishing procedures for the proper destruction of documents and electronic storage media containing personal information;
- Developing a vendor management program to ensure that vendors are trustworthy, adequately safeguard personal information, and are subject to contractual obligations to do so;
- Training authorized personnel, in coordination with the IT department, on the policy's requirements and on how to recognize a security breach and what to do when one occurs.

The State of Connecticut has taken a hard line with respect to consumer and employee protections. Employers should not be surprised to find the same is true with this new data protection legislation.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Chair of Littler Mendelson's Privacy & Data Protection Practice Group. He maintains a blog on employment related privacy issues at http://privacyblog.littler.com. Kate H. Bally is an Associate in Littler Mendelson's Stamford, Connecticut office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Mr. Gordon at pgordon@littler.com or Ms. Bally at kbally@littler.com.
