HUNTON & WILLIAMS

CLIENT ALERT

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Additional Lawyers
Utaukwa B. Allen
Cédric Burton
James A. Harvey
Jörg Hladjk
Natalie Hunt
Elizabeth Hendrix Johnson
Christopher Kuner
Manuel E. Maisog
Melinda McLellan
Randall S. Parks
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Bridget C. Treacy
John W. Woods, Jr.

Center for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

Connecticut Adopts A Comprehensive Information Security Law

In an effort to combat identity theft, Connecticut recently enacted an information security law that contains unique provisions regarding the management of Social Security numbers ("SSNs"). The law becomes effective October 1, 2008.

The law requires companies to publish an SSN protection policy. Businesses that fail to meet the law's requirements may face civil penalties up to $500,000. Similar laws in Michigan and Texas also require that companies develop SSN privacy policies.

Scope of the Law

Connecticut's information security law applies to "any person in possession of personal information of another person . . . ." For purposes of the law, "personal information" is information that is capable of being associated with a particular individual through one or more identifiers including an 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. Companies subject to the law must act to safeguard not only the specifically enumerated data elements, but any information in their possession that is capable of being associated with a

particular individual. Importantly, the law applies to personal information retained in any medium, including both computerized and hard-copy records.

A Duty to Safeguard Personal Information

The new data protection law provides, in relevant part, that entities subject to the law must act to protect personal information from misuse by third parties. This obligation extends for the duration of the information's lifecycle. Personal information must be securely maintained and, when no longer required for business purposes, disposed of securely by destroying, erasing or otherwise rendering the information unreadable.

Establish an SSN Privacy Protection Policy

The Connecticut law also creates a specific obligation for individuals and businesses that collect SSNs in the course of business to create a privacy protection policy. The policy must (i) protect the confidentiality of SSNs, (ii) prohibit the unlawful disclosure of SSNs, and (iii) limit access to SSNs. Once a privacy protection policy is established, the law requires its publication or public display. For purposes of the law, public

display includes posting the policy on an Internet web page.

Recommended SSN Protection Practices

In light of the obligations imposed by Connecticut's new law, companies that maintain personal information would be well-advised to review their personal information practices and, if appropriate, develop new privacy and information security policies and training programs to comply with the strict requirements of the new Connecticut law. In addition, companies that collect SSNs must publish or publicly display a privacy protection policy to inform individuals how SSNs are secured.

We Can Help

Hunton & Williams' Privacy and Information Management practice assists clients in developing, implementing and evaluating privacy and information security programs. If you would like assistance in reviewing your entity's privacy practices or developing new policies or training programs, please contact us.