

**NEW CONNECTICUT LAW PROTECTING PERSONAL INFORMATION AND
SOCIAL SECURITY NUMBERS REQUIRES ACTION**

In response to several well publicized incidents and heightened concern about identity theft, **effective October 1, 2008**, Connecticut will have a new law that requires business entities and individuals who possess “personal information” about another person to safeguard and properly dispose of it. This new statute, Connecticut Public Act 08-167 entitled “**An Act Concerning the Confidentiality of Social Security Numbers**” (the “Act”) will require action on the part of most businesses and many individuals. The Act specifically requires business entities and individuals to protect personal information, which is defined as any information that associates a particular individual with a unique identifier such as: 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. Personal information does not include information that is lawfully available to the general public from government records or widely distributed media.

The Act gives special attention to Social Security numbers. It requires any person who collects Social Security numbers “in the course of business” to establish and publicly display a “privacy protection policy.” The Act does not provide a sample privacy protection policy nor is there guidance other than that the policy must: (1) protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers. The Act also does not define what it means to publish or “publicly display” the privacy protection policy, but does note that one acceptable method of public display includes posting on an Internet web page.

The Act provides civil penalties of \$500 for each violation, up to a maximum of \$500,000 for any single event. “Unintentional” actions do not violate this statute. Although the penalties only apply in the case of intentional violations, the Act may put one in the position of having to prove that an action was unintentional.

The new law’s sweeping language covers not only employers and consumer transactions, but also smaller, more private deals. For example, it arguably covers the landlord who receives a tenant’s personal information, or even the colleague who collects personal checks for a child’s fundraiser.

The Act impacts all businesses that collect Social Security numbers and other personal information. The fact that all businesses that have employees must collect Social Security numbers in order to deduct FICA and other employment taxes means that all businesses must develop and follow the requirements of the new Act. Businesses must react to this statute in a very short time period, and there is little guidance from the state on such issues as the best practices for data maintenance and disposal, or what it means to “publish” a privacy protection policy. Although the new law serves the laudable purpose of preventing and deterring identity theft, it will take some time for the details of the new Act to develop. The Department of Consumer Protection will be primarily responsible for enforcing the Act although certain State agencies that issue licenses, registrations or certificates will be responsible for their own enforcement.

The following are steps that businesses and individuals should take to comply with the new statute:

1. Be alert to new developments explaining the new statute.
2. Develop a policy for the safeguarding and proper disposal of any personal information as defined above.
3. If the business or individual collects Social Security numbers, publish or display a privacy protection policy that defines how the entity protects and limits access to Social Security numbers. Make sure the policy is consistent with the existing Connecticut statute that limits the display or posting of an individual’s Social Security number. (Conn. Gen. Stat. § 42-470). That statute already prohibits such actions as printing a person’s Social Security number on a card used to access services, or requiring an individual to transmit a Social Security number over the Internet unless the connection is secure and the number is encrypted.
4. Limit physical and electronic access to any personal information governed by the Act. Make sure personnel with such access are appropriately screened and trained.
5. Develop sound practices or engage a reputable firm to store and destroy personal information properly and thoroughly. Install encryption software as appropriate on computers containing personal information.
6. If the business or individual has obligations to safeguard information under the federal Health Insurance Portability and Accountability Act (HIPAA) or other similar statutes, make sure that the new policy is consistent with the HIPAA requirements and other such privacy statutes.

In summary, this new Act will require almost every business – and many individuals – to take prompt action to safeguard the privacy of the information of their employees, customers and others.

C A R M O D Y & T O R R A N C E L L P

www.carmodylaw.com

Attorneys at Law

50 Leavenworth Street
P.O. Box 1110
Waterbury, CT 06721-1110
203.573.1200
203.575.2600 fax

195 Church Street
P.O. Box 1950
New Haven, CT 06509-1950
203.777.5501
203.784.3199 fax

Heritage Village Commercial Center
Professional Building, Suite 1C2
Southbury, CT 06488-1699
203.264.7882
203.264.7847 fax