

**September 2008**

**NEW CONNECTICUT LAW ON**  
**PROTECTION OF CUSTOMER AND EMPLOYEE DATA**

On October 1, 2008, a new Connecticut statute, Public Act 08-167 (the "Act"), will require both individuals and businesses that possess personal information to establish safeguards for such information and, if Social Security numbers are collected, to publish a specific privacy protection policy for Social Security numbers. The Act joins a nationwide trend of increasingly stringent federal and state statutes and regulations designed to protect consumers against identity theft. With less than a month before the Act takes effect, now is the time to review your company's privacy procedures and, if necessary, publish your privacy policy.

The Act imposes a broad mandate that any person in possession of personal information safeguard that information from misuse by third parties and destroy, erase or make unreadable such data prior to disposal. "Personal information" is defined as any non-public information capable of being associated with a particular individual, excluding publicly available information that is lawfully made available from federal, state or local government records or widely distributed media. The Act gives the following examples of "personal information":

- Social Security numbers
- driver's license numbers
- financial account numbers
- passport and alien registration numbers
- credit and debit card numbers
- health insurance identification numbers.

The Act also requires that every person subject to Connecticut law that collects Social Security numbers in the course of business create and publish or publicly display a privacy protection policy. The policy must ensure the confidentiality and prohibit the unlawful disclosure of the Social Security numbers. Because this requirement includes the collection of Social Security numbers from employees as well as customers, almost every Connecticut business will need to publish the details of how it protects this information. Intentionally failing to comply with the Act is punishable by a fine of \$500 for each violation up to a total of \$500,000 for a single event.

The protection of consumers' personal information has become a national concern. The Act joins many other federal and state statutes and regulations that place a duty on companies to safeguard their customers' personal information. For example, Georgia and California have previously passed laws with some provisions similar to the Act. Increasingly, the Federal Trade Commission has been fining companies that fail to protect their customers' data under its authority to regulate unfair trade practices. When a breach in data security occurs, Connecticut and 43 other states now require businesses to notify their customers of the breach. Even in the absence of government mandates, keeping employees' and customers' data secure is beneficial for both public relations and the bottom line. Notably, stock analysts estimate that the theft of TJ Maxx's electronic credit card files by a hacker will ultimately result in over \$1 billion in costs to the company.

The Act is broadly worded and as of yet there are no regulations that further define the Act's requirements. However, below are some suggestions to help companies comply with the Act:

- Identify what personal information your company collects and where the information resides (hard copies, servers, desktops, laptops, flash memory drives, CD-ROMS, backup tapes, etc.).
- Identify what external and internal risks could result in the disclosure of the information (for example, loss of a laptop by an employee, theft of data by an employee or an intrusion by a hacker).
- Create written procedures that limit these risks and provide training to your employees to implement the procedures. Designate one or more administrators to update and enforce these procedures.
- If you collect Social Security numbers, the Act requires that you publish or publicly display a privacy protection policy. The policy should describe the measures taken to protect the confidentiality of the Social Security numbers and a description of how the Social Security numbers are used. The Act suggests placing a copy of the policy on your website as a possible publication method, but does not provide further guidance. If you collect only employee Social Security numbers, we recommend providing each employee with a copy of the policy either separately or as part of an employee handbook. If you also collect customer Social Security numbers, as an alternative to placing a copy on your website, we believe mailing your customers a copy would also serve as sufficient publication with respect to your customers.
- If customers will be sending personal data to you via the Internet, ensure that the transmission is encrypted. (Nevada requires it, and it is a common sense protection for your customers.)
- Ensure that hard copies containing personal information are thoroughly shredded before disposal. Personal information stored on electronic media should be erased and made unusable. (Remember that simply hitting "delete" does not by itself erase the data from a computer hard drive.)
- Contractually require any vendors with whom you share your customers' or employees' personal information to take similar precautions.

Contact us for assistance in developing a privacy policy. We have developed some sample forms that can be tailored to a specific company's needs. If you have questions or would like further assistance regarding the Act or privacy protection in general, please contact **Patricia Weitzman** or **Russell Anderson** of our office at 203-222-0885.