

Security Alert

July 2008

NEW CONNECTICUT LAW MANDATES SAFEGUARDS FOR PERSONAL INFORMATION AND SOCIAL SECURITY NUMBERS

DUTY TO SAFEGUARD PERSONAL INFORMATION

Effective October 1, 2008, Connecticut will require both individuals and businesses that possess personal information of others to put in place safeguards to protect that information from misuse by others. The new law (Public Act No. 08-167) will require the implementation of general protection and disposal policies and procedures as to all personal information. In addition, special requirements regarding Social Security numbers will be imposed on companies and individuals that collect them in the ordinary course of business. Individuals and companies who will be subject to the new law are advised to adopt new or revised policies to comply with the new law prior to its effective date. Intentional violations of the law may result in civil penalties of \$500 for each violation and up to \$500,000 for any single event.

WHAT IS “PERSONAL INFORMATION”?

Personal information is non-public information which is associated with a specific individual through one or more identifiers. Examples include driver's license numbers, state identification numbers, credit or debit card numbers, passport numbers, health insurance identification numbers, alien resident numbers and Social Security numbers.

SPECIAL PROVISIONS FOR COLLECTORS OF SOCIAL SECURITY NUMBERS

Businesses which collect Social Security numbers must create a privacy protection policy that is published or publicly displayed, such as on a web page or it must be documented as part of any materials used to obtain Social Security numbers. The policy must:

- protect the confidentiality of the Social Security numbers,
- prohibit the unlawful disclosure of the Social Security numbers, and
- limit access to stored Social Security numbers.

DISPOSAL OF “PERSONAL INFORMATION”

The new law not only requires safeguarding of personal information, but also requires effective disposal of documents and computer files containing the personal information. Physical shredding and other



secure disposal methods are likely to be required in lieu of “reversible” erasure. Proper tracking, control and disposal of physical and electronic copies will be an important part of an effective disposal policy.

RELATED LAWS ON PROTECTION FOR SOCIAL SECURITY NUMBERS AND BREACHES INVOLVING PERSONAL INFORMATION

A related existing Connecticut Law, Conn. Gen. Stat. § 42-470, provides that collectors of Social Security numbers may not directly disclose them to the public and are prohibited from indirectly exposing them to disclosure by:

- printing an individual's Social Security number on a card that the person must use to access products or services;
- allowing unencrypted transmissions over an unsecured network (including the internet) of an individual's Social Security number; or
- requiring an individual to use his or her Social Security number to access an internet website, unless a password or unique personal identification number or other authentication is also required to access it.

Also, another existing Connecticut law, Conn. Gen. Stat. § 36a-701b, requires persons who conduct business in Connecticut and who maintain personal information to notify the affected Connecticut residents of a security breach of their personal information. Personal information is defined somewhat differently for this law, but overlaps with the new Public Act No. 08-167 mentioned above. Certain exceptions exist for personal information which has been encrypted or otherwise rendered unreadable or unusable. If the data breach affects residents outside Connecticut, the business must also comply with the laws of the other states of those affected. Some states require notice to an applicable state agency. Failure to comply with this law constitutes an unfair trade practice and is enforceable by the Attorney General for the State of Connecticut.

QUESTIONS OR ASSISTANCE?

If you have any questions about collection, safeguards and disposal plans for personal information, how to plan effectively to limit the risk of a personal information data breach, or how to deal with a breach if it should occur, please feel free to contact John Kreitler at (860) 251-5119 (jkreitler@goodwin.com) or Catherine Intravia at (860) 251-5805 (cintravia@goodwin.com). **To learn more about this topic, look for an invitation to our upcoming Personal Information Privacy Seminar.**

This communication is being circulated to Shipman & Goodwin LLP clients and friends. The contents are intended for informational purposes only and are not intended and should not be construed as legal advice. This may be deemed advertising under certain state laws. Prior results do not guarantee a similar outcome. © 2008 Shipman & Goodwin LLP.



SHIPMAN & GOODWIN LLP®

C O U N S E L O R S A T L A W

One Constitution Plaza
Hartford, CT 06103-1919
(860) 251-5000

300 Atlantic Street
Stamford, CT 06901-3522
(203) 324-8100

289 Greenwich Avenue
Greenwich, CT 06830-6595
(203) 869-5600

12 Porter Street
Lakeville, CT 06039-1809
(860) 435-2539

www.shipmangoodwin.com