

New York Enacts Statutory Protection for Confidentiality of Social Security Numbers

By [Carol Maue](#), Esq.

In recognition of the ever-increasing threat of identity theft, effective January 3, 2009, the New York General Business Law was revised to enact Section 399-dd (Confidentiality of Social Security Account Number) providing for the first time statutory protection for the confidentiality of social security account numbers to New York state residents.

The statute specifically authorizes the New York State Attorney General to enforce the new law, empowering the Attorney General to seek an injunction when a violation has occurred to restrain the offender from continued disclosure on behalf of the people of the State of New York without the necessity of demonstrating actual harm.

In addition, Section 399-dd of the General Business Law authorizes the Attorney General to seek restitution and very significant, monetary civil penalties. A first offense may result in a civil penalty of not more than one thousand dollars for a single violation and not more than one hundred thousand dollars for multiple violations from a single act or incident; a second violation or any violation committed thereafter may result in a civil penalty of not more than five thousand dollars for a single violation and not more than two hundred and fifty thousand dollars for multiple violations resulting from a single act or incident.

The law applies to “any person, firm, partnership, association or corporation” with the exception of “the state or its political subdivisions” and expressly prohibits: (i) a communication by a third party to the general public in any manner of an individual’s social security account number; (ii) any printing of an individual’s social security number on any card or tag required for the individual to access products or services or benefits; (iii) any requirement for the transmission of an individual’s social security number over the Internet unless the connection is secure and the social security number is encrypted; (iv) any requirement that an individual use his or her social security number to access an Internet website unless a password or unique personal identification number or other authentication device is also required; (v) printing of an individual’s social security account number on any materials that are mailed to the individual unless state or federal law requires the social security number to be included in the mailing and then only if mailed in a sealed envelope where the social security account number is not visible or (vi) encoding or embedding a social security number in a card or document via a bar code, chip, magnetic strip or use of any other technology in lieu of removing the social security account number as is otherwise required by the statute or (vii) filing another person’s social security account number with any public body for public inspection unless that person is a dependent, minor child of the filer or the filer has the consent of

the affected individual or the filing is otherwise mandated by federal or state law or court rule.

The new law also requires that any person or entity in the possession of any social security account numbers maintained legally for the conduct of business to take “reasonable measures” to ensure that access to the social security account numbers is limited to only those individuals who are actually required to have access to conduct such business and to provide “necessary and appropriate safeguards” to protect their “confidentiality” and to “preclude unauthorized use or disclosure.”

Provided that such safeguards have been implemented, the law does provide a safe harbor, but only in the event that the violator can prove by a “preponderance of the evidence” that the violation was unintentional and resulted from a bona fide error made notwithstanding “the maintenance of procedures reasonably adopted to avoid such error.”

The new law also specifically states that compliance with the new law may not be waived by the affected individuals; any such purported waiver “is contrary to public policy and is void and unenforceable” pursuant to Section 399-dd(5) of the GBL.

Collection of social security numbers is a common practice routinely employed by most businesses today, including health care providers, insurance companies, banks and other financial institutions, employment agencies and employers.

While a business may be protected from an inadvertent violation and significant financial sanctions provided that the safe harbor requirements are met, i.e., the alleged violator can prove both that it implemented and maintained a process reasonably adopted to avoid such error and that the violation was inadvertent and a bona fide error, routine collection of social security account numbers presents a significant risk management issue.

To the extent that a practice other than collection of social security account numbers can be utilized, most businesses would be wise to implement such measures immediately. If collection of social security account numbers is required for business operations, then adoption and maintenance of a process designed to keep such information confidential and avoid inadvertent disclosure is critical.

For more information, please contact Carol Maue at csma@cdblawyers.com

The purpose of this publication is to alert you to legal updates and developments. This is a general informational update and should not be considered legal advice.

ChamberlainD’Amanda is a full-service law firm, serving the needs of individuals, businesses and labor in Rochester, Canandaigua and Penn Yan, New York.

Copyright 2010 by Chamberlain D’Amanda Oppenheimer & Greenfield LLP. All Rights Reserved