GONZALEZ SAGGIO HARLAN

The GSH 60-Second Memo

July 1, 2009

Sponsored by the GSH Employment Group

Angela K. Dorn, Esq.

www.gshllp.com

(212) 601-2740

Want more Information on this topic?

Protecting Social Security Numbers in the Workplace

By Angela K. Dorn, Esq.

In the United States, an individual's social security number is the ultimate identifier. Crafty - and unscrupulous - individuals can access a great deal of critical, private information with a social security number. A second reality in today's world is that the use of social security numbers is ubiquitous. As each person is issued their own unique number, it has been very inviting for colleges, medical institutions, and employers to use them as their own identifiers.

Many employers regularly use employee social security numbers for such personnel purposes as conducting background checks and providing employees with benefits. However, employers are advised to safeguard the social security numbers of their employees, especially as more and more states are passing legislation to punish private entities that collect social security numbers and do not properly protect them.

CLICK HERE!

Both state and federal law can provide guidelines in this area. For example, the federal Privacy Act requires - among other things - that federal, state and local governments receive permission from an individual before releasing his or her social security number. Further, at present, more than 35 states have some sort of a social security number protection law in place.

A good example of state social security number legislation is the New York Social Security Number Protection Law. NY Gen. Bus. Law sec. 399-dd. The law places regulations on company communications and it is intended to prevent misuse and potential release of social security numbers as a result of their use in the work place. Generally, the statute regulates two activities: (i) the communication of social security numbers; and (ii) the maintenance of records containing social security numbers. While many companies are aware of the law, not all have fully implemented workplace guidelines to ensure compliance with the law.

The New York law specifically prohibits the following uses of social security numbers:

1. Any intentional communication of a social security number to the general public;
2. Printing an individual's social security number on an access card or tag that is necessary to access services, benefits or products (a building access code would likely fall under this);
3. Requiring an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted;
4. Requiring a social security number or a derivative thereof to be used as an access code for authorization purposes, such as access to a website; or
5. The mailing of materials displaying an individual's social security number, unless mandated by federal or state law.

In addition to regulating communications containing an individual's social security number, the New York law requires companies to adopt reasonable measures to limit employees' access to social security numbers in their possession. Employees with access to social security numbers must have a legitimate business purpose for doing so. Companies must store social security numbers in a manner designed to preclude unauthorized access and to ensure confidentiality. Adherence to these security measures is a defense against alleged violations of the unsecured communication obligations noted above, if in fact a crafty - and unscrupulous - individual manages to circumvent the company's defenses.

Violations of the New York law can result in serious consequences. In those cases where a company is found to have acted unlawfully, civil fines can be imposed. First-time violators can be charged $1,000 per disclosure, with a maximum of $100,000

for multiple violations from a single incident. Second-time violators face a $5,000 fine for each violation, and $250,000 for multiple violations from a single incident. Imposition of these penalties can occur even if the individual whose social security number was compromised did not suffer personal harm.

Allegations of noncompliance with the New York law may be disputed on several fronts, including by presenting evidence that social security numbers were revealed "unintentionally" or by showing that "reasonable measures" were put into effect to restrict access to social security numbers.

The most prudent action, however, is for an employer to take affirmative steps to reduce the chances of a social security number violation under the law. Such steps include:

1. Thoroughly and regularly reviewing when the company accesses employee social security numbers, how and where the numbers are stored, and reviewing procedures in place to protect the confidentiality of those numbers.

2. If the company, or a department therein, has been found to be using social security numbers as an employee identification number to facilitate access to facilities, services, or benefits, the practice should be changed immediately.

3. Similarly, an evaluation of Internet-use protocol is necessary to determine whether a company (or one of its vendors) should change its Internet authentication process to remove reliance on social security numbers. If social security numbers are used solely for authentication purposes or printed on identification tags, an alternative identifier or access code must be issued, such as a unique set of numbers unrelated to an individual's social security number.

4. Companies should ensure that their Internet connections are secure, and that whenever employee social security numbers are used on the Internet, the numbers are encrypted.

5. Limit employee access to social security numbers to a "need to know" basis, and have those employees use passwords and other techniques to ensure that they are the only individuals with access to the programs containing social security information.

6. Train employees on the importance of ensuring the confidentiality of social security numbers, as well as the costs associated with the use or dissemination of such information in violation of the law.

7. Consider updating your employee handbook to include a policy against the inappropriate access to or distribution of social security information.

Arizona
California
Illinois
Indiana
Iowa
Nevada
New York
Ohio
Washington D.C.
Wisconsin

www.gshllp.com

Lastly, whenever possible, companies should employ technological measures to use, store, and communicate social security numbers in full compliance with the legislation of each state in which it has employees.