



### SOCIAL SECURITY NUMBER PROTECTION LAW

Effective January 1, 2008, the New York Social Security Number Protection Law makes it illegal for people (including corporations and partnerships) to disclose intentionally a client's social security number ("SSN") to the public. The law also requires people, corporations and partnerships to protect the confidentiality of their client's SSN by restricting the use and disclosure of client SSN – even the use and/or disclosure of part (like the last four digits) of a client's SSN.

The Law regulates four means of disclosure to reduce the possibility of identity theft; (i) communications to the public; (ii) access cards used for services, benefits and products; (iii) use of SSN over the Internet; and (iv) mail correspondence.

1. Communications to the Public. All intentional communications, oral and/or written, of a client's SSN to the general public is prohibited. An individual may disclose his/her own SSN, but the organization that serves the individual may not.
2. Access Cards used for Services, Benefits, and Products. The Law prohibits issuing membership/benefits/access cards that display an individual's SSN. Even identification cards issued to clients or employees must not include their SSN, or any such portion.
3. Use of SSN over the Internet. The Law prohibits requiring clients (or employees) to transmit their SSN over the Internet, unless the SSN is encrypted or the Internet site is secure. A SSN can no longer serve as the sole means of identity authentication, e.g. using a client's SSN (or a portion of their SSN) as the password to access their benefits via a website.
4. Mail Correspondence. Though several exceptions exist<sup>1</sup>, the Law prohibits the mailing of materials with client's SSN printed within.

The Law also sets limits on how an organization uses SSNs for internal purposes. An organization must limit employee access to client SSNs except when an employee has a legitimate business need for access<sup>2</sup>. Employee access to client SSNs must be kept to an absolute minimum. Every effort should be made to ensure that client SSNs are stored in a manner that prevents illegal use by employees, and/or disclosure to the public.

Organizations should undertake an analysis of whether it is necessary to obtain client SSNs and the safeguards they can adopt to protect this information.

---

<sup>1</sup> Exceptions include: (i) documents mandated by Federal or State Law to have an individual's SSN; (ii) forms or applications, including those used to establish or cancel accounts, so long as the SSN is contained inside a sealed envelope and cannot be viewed unless the envelope is opened.

<sup>2</sup> The Law does not define "legitimate business need".

## **PENALTIES**

The Law grants enforcement powers to the New York State Attorney General's Office, who will initiate a claim in civil court against violating organizations. Civil penalties for first-time violators range from \$1,000 per violation, to a maximum of \$100,000 for multiple violations resulting from a single incident<sup>3</sup>. Second-time violators face penalties of \$5,000 per violation, with a maximum of \$250,000 for multiple violations resulting from a single incident.

*This alert is meant to provide general information only, not legal advice. The Social Security Number Protection Law contains specific requirements and details not included here. If further information is desired please contact Staff Attorney Viva Obioha at Lawyers Alliance for New York at (212) 219-1800 x 276 for further information.*

Lawyers Alliance for New York is the leading provider of business and transactional legal services for nonprofit organizations that are improving the quality of life in New York City neighborhoods. Our network of pro bono lawyers from law firms and corporations and staff of experienced attorneys work together, delivering expert corporate, tax, real estate, employment and other legal services to community organizations. By connecting lawyers, nonprofits and communities, we help nonprofits to develop affordable housing, stimulate economic development, and operate vital programs for children and young people, the elderly, recent immigrants, and other low-income New Yorkers.

---

<sup>3</sup> An example of multiple violations arising out of a single incident is if a hacker were to gain access to multiple SSNs at once due to an illegal use or disclosure of a client's SSN, or improperly secured data containing client SSN.