LEGGE, FARROW, KIMMITT, McGRATH & BROWN, L.L.P.

KATHERINE T. MIZE
BOARD CERTIFIED LABOR AND EMPLOYMENT
TEXAS BOARD OF LEGAL SPECIALIZATION
kmize@leggefarrow.com

ATTORNEYS AT LAW
6363 WOODWAY
SUITE 400
HOUSTON, TEXAS 77057
(713) 917-0888
www.leggefarrow.com

DIRECT
(713) 706-4904
FACSIMILE
(713) 953-9470

September 4, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex K)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Via Federal Express

Re: SSNs in the Private Sector – Comment Project No. P075414

Dear Secretary Clark:

We write on behalf of a client of our firm to address certain issues raised by the use of Social Security numbers ("SSNs") as employee identifiers. Our client is a corporation which provides goods and services in connection with the development of our nation's energy resources. Our client does not wish to be identified by name.

The extensive collection and use of SSNs as an employee identifier has exposed individuals to considerable risk of misuse of those numbers. Identity theft is one form of such misuse, but there are others. An individual's SSN is often used to gather information about a job applicant or contractor in connection with decisions regarding employment, access to a work location, or other purposes. Although the Fair Credit Reporting Act ("FCRA") is meant to prevent misuse of such information by regulating how information is gathered through credit reporting agencies (as defined in the FCRA), that statute does not prevent a party from requiring a consent to unlimited use and disclosure of information obtained. Although the FCRA attempts to limit this practice, its limitations do not expressly extend to use of outdated information compiled over time and made readily accessible by use of SSNs as the personal identifier. 15 U.S.C. § 1681b(b).

As you know, Congress enacted the Privacy Act in 1974 to limit and control governmental use of personal information. *See* 5 U.S.C. § 552a ("the Privacy Act"). The Privacy Act provides that no governmental entity may deny any rights to an individual based on his or her refusal to disclose his or her SSN: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security account number." Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(1), *reprinted in* 5 U.S.C. § 552a note (2007). However, the statute provides an exception when production of SSNs is required by federal statute. Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(2), *reprinted in* 5 U.S.C. § 552a note (2007). When that is the case, the "Federal, State or local government agency which requests an individual to disclose his

Social Security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." Privacy Act of 1974, Pub. L. No. 93-579, § 7(b), *reprinted in* 5 U.S.C. § 552a note (2007). A general exception to these requirements exists if an individual consents to disclosure of the information. 5 U.S.C. § 552a(b).

At present, federal law does not appear to prohibit a private company contracting for services from requiring disclosure of SSNs of the contractor companies' employees' as a condition of access to a work site or eligibility to perform the contracted services. Under federal law, an employer may be able to lawfully require disclosure of the employee's SSN to a third party as a condition of employment. This means that a contracting company could obtain and use SSNs to identify and deny facility access to workers it deems ineligible based on criteria derived from or tied to SSNs. While federal (and state) employment laws generally protect workers from discrimination or retaliation by their actual or prospective employer, those laws generally do not protect workers from decisions with employment-related impact which are made by non-employers. This means that a contracting company could use information derived from the use of SSNs to influence the relationship between an employee and his or her employer.

For example, a contracting company could potentially refuse access to a contractor's employee based on his past assertion of a workers' compensation claim, or his filing of a charge of discrimination, or his protected status under the Americans With Disabilities Act. Doing so would effectively preclude the contractor from employing the worker as intended and would likely have the effect of forcing the contractor to reassign or not employ the worker. In effect, SSNs may be used to identify or track information about employee populations which may be used indirectly to discriminate or retaliate against employees who would otherwise enjoy protected status. Disallowance of the use of SSNs as an employee identifier would make this scenario considerably less likely as it would make it more difficult for companies to gather and maintain databases of information which might be used in this regard.

In the wake of 9/11, and in response to calls by the Department of Homeland Security for heightened security at industrial facilities, many operators of industrial facilities have begun requiring individuals who access their facilities (either as contractors' employees or as business visitors) to present multiple forms of identification, even in the absence of laws or regulations requiring them to do so. Contractors are increasingly being asked to provide advance listings of employees assigned to particular jobs or sites which include SSNs and other information which could be used in connection with identity theft. Because there are no uniform standards for how this private information may or must be handled or used, the potential for misuse or loss of the information is significant. Disallowance of the use of SSNs as a public identifier would significantly reduce that risk. In addition, in light of the provisions of the Privacy Act requiring identification as to whether disclosure of information is mandatory, a rule requiring private companies who gather information pursuant to federal law to disclose the basis for their collection of the information would be appropriate.

Employers are currently required to maintain employee medical records separate from employee personnel files for privacy reasons. Employers also maintain separate files for employment eligibility verification documents (I-9s). Our client does not believe limiting employer use of SSNs to just wage tracking and reporting would work a significant hardship on employers. Our client maintains an HRIS system in which it tracks employee data, including SSNs. Although our client would incur cost in transitioning away from use of SSNs as identifiers, our client views that cost and the cost and administrative effort to maintain its records as minimal.

Our client suggests that the most sensible approach would be for employers to be permitted to use SSNs for wage reporting and tax withholding purposes, but not for other purposes. Our client would also support reasonable rules relating to the protection of such information, and prohibitions on the use or communication of SSNs for employment-related purposes. Because of the possible misuse described above, our client also supports rules which would preclude an employer from requiring an employee to consent to broader use of SSNs as a condition of employment.

Our client supports enactment of clear, bright-line rules limiting the public use of SSNs. Our client believes doing so will reduce the incidence of identity theft and prevent SSNs from being used for other purposes inconsistent with established law. It is our client's position that limiting use of SSNs to use as an internal identifier for wage withholding purposes will not work an undue hardship on employers and will bring stability and reduce risk.

Thank you for your thoughtful consideration of these issues.

Very truly yours,

Katherine T. Mize
Laurence E. Stuart