



To All Clients

November 4, 2005

## **MICHIGAN SOCIAL SECURITY NUMBER PRIVACY ACT**

### **REQUIRES FORMAL PRIVACY POLICY BY JANUARY 1, 2006**

**As of January 1, 2006**, the Michigan Social Security Number Privacy Act will require all entities with Michigan-based employees or that deal with Michigan-based vendors or persons working for any Michigan-based business to develop a formal privacy policy applicable to all such Michigan-based employees and businesses. The privacy policy must detail the security practices and procedures adopted to protect the confidentiality of the social security numbers (SSNs) of such businesses and individuals. Under the Act, SSNs are considered to be the most confidential form of sensitive personal information. The law applies without regard to where the affected business is incorporated or headquartered; for example, an Indiana entity dealing with Michigan-based vendors will be subject to the Act.

Although the Act became effective on March 1, 2005, the privacy policy must be implemented and distributed to employees and other persons on or before **January 1, 2006**.

The Act does not specify all of the procedures that must be included in the required privacy policy. The standard principals of privacy and disclosure should, however, apply, including disclosure of how an SSN will be collected, used, stored and/or maintained; disclosure of third party access or use of an SSN; and a description of the safeguards that will be in place to prevent the unauthorized use of or access to an SSN. The privacy policy must be published in an employee handbook, manual or similar document, and it can also be made available electronically, such as by posting it on a website or distributing it by e-mail.

The Act requires the implementation of certain safeguards regarding the use and display of four or more numbers of an SSN:

- ❖ A business must ensure, to the extent

practicable, the confidentiality of employee and other business associate SSNs and prohibit unlawful disclosure of SSNs;

- ❖ A business must limit who has access to information or documents containing SSNs;
- ❖ A business must establish a document destruction protocol for those documents containing SSNs; and
- ❖ A business must impose penalties on employees, agents, representatives, or service providers who violate the business' privacy practices.

Additionally, a business may not:

- ❖ Publicly display more than four sequential digits of an SSN;
- ❖ Use more than four sequential digits of an SSN as the primary account number for an individual;
- ❖ Visibly print more than four sequential digits of an SSN on any identification badge, card, membership card, permit, or license;
- ❖ Require an individual to use or transmit more than four sequential digits of his/her SSN over the internet, computer system, or network unless the connection is secure or the transmission is encrypted;
- ❖ Require an individual to use or transmit more than four sequential digits of his/her SSN to gain access to an Internet website, computer system, or network unless the connection is secure, the transmission is encrypted, or a password (or other unique personal

identification number or other authentication device) is also required to gain access to the Internet website, computer system, or network;

- ❖ Include more than four sequential digits of the SSN in or on any document or information mailed to an individual if it is visible on, or from the outside of the envelope or packaging; and
- ❖ Include more than four sequential digits of the SSN in any document or information mailed to a person, unless state or federal law, rule, regulation, or court order authorizes, permits, or requires that the social security number appear in the document, the document is sent as part of an application or enrollment process, or the document is sent to establish, confirm the status, amend, or terminate an individual's health insurance benefits.

The Act requires the proper disposal of information (in any written, electronic, or other form) that contains SSNs. Such disposal must make SSN information unreadable, undecipherable, or not able otherwise to be practicably reconstructed. Other states, including California, Nevada, New Jersey, North Carolina, and Texas, and the Federal Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act of 2003, also require the disposal of sensitive personal information in a secure manner.

Failure to comply with the Act's security requirements is punishable by criminal penalties, including imprisonment, a fine, or both, for willful violations, and creates a private right of action by employees, vendors and business associates.

Although this is the first such law of its kind to require a formal privacy policy for employees

and business associates, and is applicable only to activities involving Michigan companies and/or personnel, this Act may prove to be a *de facto* national standard. It may ultimately not be considered reasonable for a business active in several states to create and distribute a formal privacy policy for employees and other affected persons located only in Michigan, especially since, at last count, 29 states have laws for the protection of misuse and unauthorized use of SSNs, and 22 states and New York City have enacted consumer notification requirements in the event of a security breach or alleged security breach of sensitive personal information such as SSNs.

In a related development, the Federal Trade Commission recently expanded its regulation of unfair trade practices through an enforcement proceeding against a retail company for its failure to develop and implement reasonable security practices and procedures for the protection of its customers' credit and debit card account numbers and other forms of sensitive personal information, including SSNs. BJ's Wholesale Club entered into a settlement agreement with the FTC under which BJ's is required to develop a comprehensive information security program, conduct audits of its program by an independent professional, implement extensive recordkeeping requirements, and submit to FTC oversight in this regard for 20 years. This settlement reinforces the need for all businesses to implement reasonable security practices and procedures that will reduce the risk of identity theft and the unauthorized use or access to SSNs and other sensitive personal information, or be subject to state and federal consumer protection laws plus civil lawsuits.

We recommend that you contact us to review your privacy policies and to discuss the implementation of standard security practices and procedures for all sensitive personal information.

\* \* \* \*

This memorandum is intended only as a general discussion of these issues and should not be regarded as legal advice. We would be pleased to provide additional details or advice about specific situations if desired. To discuss any of the issues presented here, please contact S. Jenell Trigg at (202-416-1090) or any other attorney in our office.