



WISCONSIN LEGISLATIVE COUNCIL ACT MEMO

2005 Wisconsin Act 138
[2005 Senate Bill 164]

**Notice of Unauthorized Acquisition
of Personal Information**

2005 Wisconsin Act 138 requires entities to notify individuals of certain unauthorized acquisitions of personal information.

Notice Requirements

The Act provides that, if an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of the personal information.

The requirements of the Act apply to entities that: (a) conduct business in Wisconsin and maintain personal information in the course of business; (b) license personal information in Wisconsin; (c) maintain for a Wisconsin resident a depository account; or (d) lend money to a resident of Wisconsin. An "entity" also includes: (a) the state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the Legislature and the courts; and (b) a city, village, town, or county.

"Personal information" means an individual's last name and the individual's first name or first initial, *in combination with and linked to* any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (d) the individual's DNA profile; and (e) the individual's

This memo provides a brief description of the Act. For more detailed information, consult the text of the law and related legislative documents at the Legislature's Web site at: <http://www.legis.state.wi.us/>.

unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical characteristic.

The Act also provides that, if an entity whose principal place of business is *not* located in Wisconsin knows that personal information pertaining to a Wisconsin resident has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each Wisconsin resident who is the subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident.

Finally, the Act provides that, if a person, other than an individual, that stores personal information pertaining to a Wisconsin resident, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the information must notify the person that owns or licenses the information of the acquisition as soon as practicable.

Under the Act if, as a result of a single incident, an entity is required to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity must without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the individuals.

An entity is *not* required to provide notice, as described above, if: (a) the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information; or (b) the personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

Timing and Method of Notification

Under the Act, an entity must provide the required notice within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination of reasonableness must include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

An entity must provide notice by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject, and if the entity has not previously communicated with the subject, the entity must provide notice by a method reasonably calculated to provide actual notice to the subject.

Upon written request by a person who has received a notice under the Act, the entity that provided the notice must identify the personal information that was acquired.

Exempt Entities

The notice provisions of the Act do not apply to financial institutions that are subject to and in compliance with federal law relating to disclosure of nonpublic personal information or a person that has

a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. In addition, the provisions do not apply to health plans, health care clearinghouses, or health care providers, if the entity complies with federal law relating to security and privacy of information maintained by those entities.

Civil Claims

Under the Act, failure to comply with the requirements of the Act is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

Law Enforcement Requests to Not Notify

Under the Act, a law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under the Act for a period of time. The notification process must begin at the end of that time period. If an entity receives such a request, it may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

Local Ordinances or Regulations Prohibited

The Act provides that no city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of unauthorized acquisition of personal information.

Effect of Federal Legislation

Under the Act, if the Joint Committee on Administrative Rules determines that the federal government has enacted legislation that imposes notice requirements substantially similar to the requirements of the Act and determines that the legislation does not preempt the provisions of the Act, the committee must submit to the Revisor of Statutes a notice of this determination to be published in the Wisconsin Administrative Register.

Effective Date: Act 138 takes effect on March 31, 2006.

Prepared by: Anne Sappenfield, Senior Staff Attorney

March 30, 2006

AS:wu