



WISCONSIN LEGISLATIVE COUNCIL INFORMATION MEMORANDUM

New Wisconsin Identity Theft Statutes (2005 Acts 138, 139, and 140)

Three acts enacted in the 2005-06 Session that attempt to reduce and prevent fraud resulting from identity theft are discussed in this report. 2005 Wisconsin Act 138 requires organizations that maintain personal information to notify the individuals to whom the information pertains when their information has been disclosed to an unauthorized party. 2005 Wisconsin Act 139 attempts to restrict the flow of Social Security numbers into certain public documents processed by registers of deeds. Finally, 2005 Wisconsin Act 140 allows Wisconsin citizens to control the release of their credit reports through the use of a “security freeze.”

Act 138: “Data security breach laws” require organizations that maintain or license personal information to, under certain circumstances, notify the individuals to whom the personal information pertains when their information has been disclosed to an unauthorized party; nearly half of the states have such laws. Wisconsin joins them in passing Act 138, which requires companies that conduct business in Wisconsin or maintain or license personal information pertaining to Wisconsin residents to notify the individuals of certain unauthorized disclosures. Because the individuals may often be at increased risk of being a victim of identity theft fraud following an unauthorized disclosure of their information, the notice serves as an alert that they should closely monitor their financial accounts and credit reports for signs of identity theft.

Act 139: Public records are a rich source of personal information for identity thieves perpetrating fraud against individuals. By prohibiting Social Security numbers from being included in certain documents recorded by registers of deeds, Act 139 attempts to restrict the availability of this type of information critical to identity thieves. To provide incentives for compliance with the statute, the Act allows individuals to seek damages from a person that drafted the offending document on behalf of the individual, such as a real estate attorney.

Act 140: Through Act 140, Wisconsin provides residents with another identity theft consumer protection measure that has been enacted in several other states – the ability for residents to control the release of their credit reports. Potential creditors will refuse to grant credit to an individual, or an identity thief attempting to fraudulently obtain credit by posing as the individual, without receiving a credit report from a consumer reporting agency. Therefore, by allowing an individual to restrict the release of his or her credit report from a consumer reporting agency to a potential creditor, certain types of financial fraud perpetrated by identity thieves can be prevented. Under the Act, an individual can place a “security freeze” on his or her credit report for a fee not to exceed \$10 for each of the three major consumer reporting agencies. The consumer reporting agency is thereafter prohibited from releasing the credit report to potential creditors unless the individual either temporarily or permanently removes the security freeze, both of which are subject to a \$10 maximum fee.

Acts 138 and 139 took effect on March 31, 2006. Act 140 takes effect on January 1, 2007.

NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION (ACT 138)

OVERVIEW AND BACKGROUND

Wisconsin Act 138, adopted in 2005, requires certain businesses, state government entities, and local governments to notify individuals of an unauthorized disclosure of their personal information.

This type of statute is often referred to as a “data security breach law.” California was the first state to enact a data security breach law following a 2002 computer intrusion in which hackers downloaded the personal information of 265,000 employees of the State of California. After becoming effective in 2003, the California law was widely credited with exposing several intrusions in which massive amounts of personal information were stolen. The largest of these intrusions was of Choicepoint, a commercial data broker, which announced that in April 2005, the personal information of 310,000 people may have been released to unauthorized individuals.

Data security breach laws in other states have helped to ameliorate the effects of personal data disasters such as commercial data broker Choicepoint's 2005 announcement of its disclosure of the personal information of up to 310,000 individuals.

Following California's lead, 22 other states enacted data security breach laws in 2005; an additional six states, including Wisconsin, passed such laws in 2006. At the time, no federal legislation addresses the issue although at least one bill is active in Congress.

NOTICE TRIGGERS

The Act creates a new section, s. 895.507, Stats., “Notice of unauthorized acquisition of personal information.” If a covered entity, which includes certain businesses, state government entities, and local governments, knows that a person has acquired personal information in the entity's possession, then the entity generally must notify the individuals whose personal information was acquired as a result of the security breach.

“Personal information” means an individual's last name and his or her first name or first initial in combination with and linked to any of the following elements, if the element is not publicly available and is not encrypted or redacted:

1. The individual's Social Security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account, 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.
4. The individual's DNA profile.
5. The individual's biometric data such as a fingerprint, voice print, or retina image.

As mentioned, if the element is encrypted or redacted, then the notification requirement fails to be triggered. However, “encryption” is not defined by the Act. Likewise, if the element is “publicly available information,” then the notification requirement also fails to be triggered. “Publicly available information” means information that is lawfully: (1) made widely available through any media; or (2) made available through public records.

Covered entities, as described below, whose principal place of business is in Wisconsin, that maintain or license personal information in this state that know of an unauthorized acquisition of personal information must make reasonable efforts to notify each subject of the personal information regardless of the state of residency of the subjects. Covered entities whose principal place of business is *outside* of Wisconsin that know of an unauthorized acquisition of personal information pertaining to a Wisconsin resident must make reasonable efforts to notify each Wisconsin resident of the acquisition. More specific notice requirements are described below.

Finally, a person that stores personal information pertaining to Wisconsin residents but does not own or license the personal information who knows of an unauthorized acquisition of personal information must notify the person that does *own or license* the personal information of the acquisition as soon as practicable.

If a law enforcement agency, in order to protect an investigation or to protect homeland security, requests an entity not to provide notices to the subjects, then the Act prohibits the entity from providing notices that would otherwise be required. The law enforcement agency may request that the entity delay notification for any length of time. After that time period expires, the notification requirements provided by the Act apply.

COVERED ENTITIES

The entities subject to the Act are persons, other than individuals, that do any of the following:

1. Conduct business in the State of Wisconsin.
2. License personal information in Wisconsin.
3. Maintain a “depository account” within the meaning of the Wisconsin civil statutes regulating creditor-debtor relationships [ch. 815, Stats.].
4. Lend money to a Wisconsin resident.

Government agencies are also covered entities, including any state office, department, independent agency, or authority as well as local governments – cities, villages, towns, and counties.

Wisconsin government agencies at all levels, including cities, villages, towns and counties, must comply with the notification requirements of Act 138.

However, certain entities that are already subject to federal data security regulations are exempt from the Act if they are in compliance with the relevant federal regulations. These include entities subject to the Gramm-Leach-Bliley Act regulating financial institutions and those subject to the Health Insurance Portability and Accountability Act (HIPAA) regulating health care organizations.

MATERIAL RISK OF IDENTITY THEFT REQUIRED

An entity is not required to notify the subject of personal information of an unauthorized acquisition of information pertaining to him or her if the acquisition does not create a “material risk of identity theft or fraud” to the subject.

NOTICE REQUIREMENTS

After an unauthorized acquisition has been discovered, the entity must send a notice to the subjects of the personal information indicating that the entity knows of the unauthorized acquisition. The notice must be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition, and must be delivered by postal mail or by any method that the entity has previously used to communicate with the subject of the data, such as email or telephone. After a subject receives a notification, he or she may request the entity to identify the personal information that was acquired.

Additionally, if the acquisition affects 1,000 or more individuals, the entity must notify the consumer reporting agencies, informing them of the timing, distribution, and content of the notices.

PREEMPTION PROVISIONS

The Act preempts local government ordinances or regulations that relate to the notice or disclosure of unauthorized acquisition of personal information.

With respect to federal preemption, if the Joint Committee on Administrative Rules determines that Congress has enacted legislation that imposes notice requirements substantially similar to those in the Act, then the committee must submit its finding to the Revisor of Statutes. After this notice is published, the statute created by the Act no longer applies.

ENFORCEMENT

The Act does not provide enforcement responsibilities to any state agency nor does it expressly allow individuals whose personal information is acquired by an unauthorized person to file a lawsuit against the entity storing or licensing the personal information.

RESTRICTIONS ON RECORDING OF SOCIAL SECURITY NUMBERS BY REGISTER OF DEEDS (ACT 139)

OVERVIEW

2005 Wisconsin Act 139 attempts to prevent individuals' Social Security numbers from being included in documents that are recorded by the Register of Deeds, such as mortgages, deeds, and real estate conveyances. Two means of enforcement are provided: (1) registers of deeds may refuse to process any document that contains a Social Security number or may remove or obscure the number; and (2) the drafter of a document that unlawfully includes an individual's Social Security number may be held liable for damages that the individual suffers because of the inclusion of the number.

By keeping Social Security numbers from being recorded on certain public records, Act 139 attempts to limit identity thieves' access to this critical information.

ROLE OF THE REGISTERS OF DEEDS

Registers of deeds have two options when presented with an instrument to be recorded that has an individual's full nine-digit Social Security number ("SSN"). Because the Act prohibits the register from recording an instrument that contains a SSN, he or she must either refuse to record the instrument or may, at the discretion of the register, remove or obscure the SSN before recording the instrument.

However, if a register does record an instrument containing an individual's SSN, he or she cannot be held liable for damages that the individual may suffer as a result of the recording (for example, from identity theft). If the register discovers the SSN on an instrument that was recorded after the effective date of Act – that is, a SSN that was not discovered during a review of the instrument before it was recorded – he or she may remove or obscure the SSN on the recorded instrument.

CIVIL LIABILITY FOR INSTRUMENT DRAFTERS AND EFFECTIVE DATE

Act 139 imposes civil liability on instrument drafters, such as real estate attorneys, for failure to remove SSNs from drafted instruments that are then recorded by a register of deeds. If a register of deeds records an instrument containing the complete nine-digit SSN of an individual, then the instrument drafter may be held liable to the individual for any actual damages resulting from the recording of the instrument.

EXCEPTIONS

The provisions of the Act do not apply to federal income tax liens, certificates of military discharge, or "vital statistics" certificates such as birth, death, and marriage certificates.

SECURITY FREEZES FOR CREDIT REPORTS (ACT 140)

OVERVIEW AND BACKGROUND

2005 Wisconsin Act 140 allows individuals to “freeze” their credit reports (referred to as “consumer reports” in the relevant federal and Wisconsin statutes and in this memorandum). If an individual places a “security freeze” on his or her consumer report, then the consumer reporting agency may not release the consumer report to a potential creditor unless the individual has first “thawed” his or her report, thus allowing the consumer reporting agency to release the report. By keeping his or her consumer report frozen, an individual can prevent an identity thief from receiving credit in the individual’s name because most creditors will not extend credit without reviewing the individual’s consumer report.

In many cases, freezing a consumer report prevents an identity thief from fraudulently gaining credit in the person’s name – without the consumer report, most creditors will not extend credit.

At the time of writing, 17 states have passed consumer report security freeze laws. Again, California was the first state to pass such a law, which became effective on January 1, 2003.

PLACING A SECURITY FREEZE

Act 140 provides that an individual may place a security freeze on his or her consumer report by mailing the request via certified mail to the consumer reporting agency (“CRA”) or via any other methods that the CRA may provide. The CRA may charge the individual up to a \$10 fee and the individual must provide the CRA with proper identification. (The fee waiver provision is described below.) The Department of Agriculture, Trade and Consumer Protection will promulgate rules specifying what constitutes “proper identification.”

Individuals should place security freezes with each of the three major CRAs – Equifax, Experian, and TransUnion – in order to be fully protected at a total cost of \$30.

Placing security freezes with each of the three major consumer reporting agencies may cost up to \$30.

OPERATION OF THE SECURITY FREEZE

Within five business days after receiving an individual’s request for a security freeze, the CRA must comply with the core requirement of the Act: the CRA may not release the consumer report to any person for any purpose related to the extension of credit unless the individual provides prior authorization for the release (see the following sections on removing a security freeze).

Additionally, within 10 days after receiving a request for a security freeze, the CRA must send the individual a notice that does all of the following:

1. Confirms the security freeze.
2. Includes a unique personal identification number (“PIN”), password or other device for the individual to authorize the release of the consumer report.

3. Describes the procedure for authorizing the release of the individual's consumer report.

TEMPORARILY REMOVING A SECURITY FREEZE

When processing an individual's application for credit, a potential creditor will nearly always require the individual's consumer report in order to evaluate his or her creditworthiness. To remove a security freeze in order to allow a potential creditor to receive the individual's consumer report, an individual must perform all of the following steps:

1. Contact the CRA using a point of contact designated by the CRA.
2. Provide proper identification and the PIN, password or other device provided by the CRA at the time of the placement of the security freeze.
3. Specify the time period for which the release is authorized.
4. Pay a fee not to exceed \$10 (unless the fee waiver applies).

Within three days after the individual meets these requirements, the CRA must remove the freeze from the individual's consumer report. After doing so, the potential creditor will be allowed to receive the consumer report and thereby evaluate the individual's creditworthiness.

PERMANENTLY REMOVING A SECURITY FREEZE

To permanently remove a security freeze, an individual must perform the same steps for temporarily removing a security freeze, as detailed immediately above.

Within three days after the individual meets these requirements for permanently removing the security freeze, the CRA must remove the freeze from the individual's consumer report. The CRA may then release the consumer report to any party that is otherwise authorized by the Fair Credit Reporting Act to receive the report.

IDENTITY THEFT FEE WAIVER

If an individual has been the victim of identity theft, then he or she may be eligible for fee waivers for security freeze placements and removals. To qualify, the individual must submit evidence to the CRA that he or she has made a report of identity theft to a law enforcement agency. If the evidence is satisfactory to the CRA, then it may not charge the individual a fee for placing, temporarily removing, or permanently removing a security freeze on or from the consumer report.

Identity theft victims are exempt from the fees associated with Act 140.

MATERIAL MISREPRESENTATION EXCEPTION

If the CRA included a security freeze with a consumer report due to a material misrepresentation of fact by the individual, the CRA may release the consumer report to a party requesting the report. However, the CRA must notify the individual in writing about the misrepresentation before the CRA releases the consumer report.

INTERPRETATION OF A SECURITY FREEZE BY A POTENTIAL CREDITOR

The purpose of restricting the release of an individual's consumer report is to prevent a potential creditor, such as a credit card company, from extending credit to an identity thief that is fraudulently attempting to gain credit in the individual's name. Without being able to receive and review the individual's consumer report due to the security freeze, a potential creditor will rarely extend credit in the individual's name.

The Act provides explicit guidance in this regard. Specifically, if a party requests access to an individual's consumer report that includes a security freeze and the request is made in connection with an application for an extension of credit, then the party may treat the individual's applications as "incomplete." The CRA is permitted to advise the requesting party that the report includes a security freeze and that the CRA must obtain the individual's authorization before releasing the report.

COVERED ENTITIES

Consumer reporting agencies, as defined in the federal Fair Credit Reporting Act, must comply with the requirements of Act 140. However, certain entities that otherwise may be CRAs under the federal law are exempt from Act 140 and include:

1. A reseller, which is a CRA that acts only as a reseller of credit information but does not maintain a permanent database of credit information from which new consumer reports are produced. However, if a reseller obtains from another CRA a consumer report that includes a security freeze, then the reseller shall include the security freeze with any consumer report regarding the individual that the reseller maintains.
2. A CRA that is a check services or fraud prevention services company.
3. A CRA that is a deposit account information service company.
4. Exceptions.

The Act is intended to prevent certain kinds of financial fraud perpetrated by identity thieves. Therefore, the security freeze provision that restricts the release of consumer reports primarily applies to potential creditors processing an individual's application for an extension of credit. However, companies and government agencies regularly use consumer reports for other purposes. Therefore, the security freeze provisions do not apply to various parties or uses including the following:

Security freezes do not prohibit all releases of consumer reports; for example, child support agencies may still access the frozen report.

1. A person with whom the individual has, or had, a prior business relationship.
2. A subsidiary, affiliate or agent of a person with whom the individual has, or had, a prior business relationship.

3. An assignee of a financial obligation owed by the individual to a person with whom the individual has, or had, a prior business relationship.
4. Any state, or local agency, law enforcement agency, court, or private collection agency acting pursuant to a court order, warrant, or subpoena.
5. A child support agency.
6. The state acting to investigate fraud or acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory requirements.
7. A credit card company providing unsolicited "pre-screened" credit card offers.
8. A person administering a credit file monitoring subscription service to which the individual has subscribed.
9. A person for the purpose of providing an individual with a copy of his or her consumer report upon the individual's request.
10. An insurer authorized to do business in Wisconsin that uses the consumer report in connection with the underwriting of insurance involving the individual.
11. A person who intends to use the information in the consumer report for employment purposes.

CONSUMER EDUCATION

Whenever a CRA is required to provide an individual with a notice under certain provisions of the federal Fair Credit Report Act, Act 140 requires that it also provide the individual with a notice about the Wisconsin security freeze provisions of the Act. Required notice language is included in the Act. The notice explains how the security freeze statute works from the consumer's perspective, including how to place and remove a freeze with a CRA. It also warns that the security freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a loan, credit, mortgage, or Internet credit card transaction, including an extension of credit at point of sale.

ENFORCEMENT

A person that fails to comply with the requirements of the Act is liable for actual damages sustained by an individual as a result of the failure, the costs of the action, and reasonable attorney fees.

TEXT OF THE LAWS

The data security breach notification requirements of Wisconsin Act 138 are found in s. 895.507, Stats. The restrictions on SSNs being included in documents recorded by a register of deeds provided by Wisconsin Act 139 are found in s. 59.43 (1m), Stats. The consumer report

security freeze provisions of Wisconsin Act 140 are found in s. 100.54, Stats. (“Access to credit reports”).

The text of the statutes and of the Acts may be accessed via the Wisconsin State Legislature’s website at <http://www.legis.state.wi.us/>. (Click on “Wisconsin Law.”)

The memorandum was prepared by Patrick Mueller, Legal Intern on July 18, 2006. The memorandum is not a policy statement of the Joint Legislative Council or its staff.

WISCONSIN LEGISLATIVE COUNCIL

One East Main Street, Suite 401 • P.O. Box 2536 • Madison, WI 53701-2536

Telephone: (608) 266-1304 • Fax: (608) 266-3830

Email: leg.council@legis.state.wi.us

<http://www.legis.state.wi.us/lc>