WISCONSIN LEGISLATIVE COUNCIL
INFORMATION MEMORANDUM

Wisconsin Laws Relating to Identity Theft

The unauthorized use of personal identifying information, commonly termed "identity theft" is prohibited in Wisconsin. Identity theft occurs when a person intentionally uses or attempts to use personal identifying information or personal identification documents of another to obtain anything of value, including credit or services.

In addition to the crime of identity theft, Wisconsin has a number of other laws intended to curb the practice. These laws include records disposal and loss notification requirements, certain restrictions on the recording of Social Security numbers, and the ability to place a "security freeze" on one's credit reports to prevent unauthorized use.

UNAUTHORIZED USE OF AN INDIVIDUAL'S PERSONAL IDENTIFYING INFORMATION

A person who intentionally uses or attempts to use personal identifying information or personal identification documents (a birth certificate, personal identification number ("PIN"), or financial transaction card) of another individual to obtain credit, money, goods, services, or anything of value, without that individual's authorization or consent, to avoid civil or criminal process or penalty, or to harm the reputation, property, person, or estate of an individual, is guilty of a Class H felony. A Class H felony is punishable by imprisonment for up to six years, a fine of up to $10,000, or both.

For the purposes of this statute, personal identifying information includes **an individual's**:

- Name.
- Address.
- Telephone number.
- Driver's license number.
- Social Security number ("SSN").
- Employer or place of employment.
- Employee identification number.
- Mother's maiden name.
- Financial account numbers.

- Taxpayer identification number.
- DNA profile.
- Any number or code that can be used alone or with an access device to obtain money, goods, services, or any other thing of value.
- Unique biometric data, including a fingerprint, voice print, retina or iris image, or any other unique physical representation.
- Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.
- Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

In addition, the law provides that if any individual reports an identity theft violation to the law enforcement agency where the individual resides, but the violation occurs outside of that law enforcement agency's jurisdiction, the law enforcement agency receiving the complaint must prepare a report on the violation and forward it to the law enforcement agency in the appropriate jurisdiction. [s. 943.201, Stats.]

RECORDS CONTAINING PERSONAL INFORMATION

Wisconsin law requires certain businesses and government entities to take actions to protect certain personal information.

DISPOSAL OF RECORDS

Wisconsin law prohibits financial institutions, medical businesses, and tax preparation businesses in this state from disposing of records that contain personal information unless the personal information is first rendered undiscoverable. The statutes provide that these businesses may discard the records only after they do one of the following prior to disposal:

- Shred the records.
- Erase the personal information contained in the records.
- Modify the records to make the personal information unreadable.
- Take actions that the businesses reasonably believe will ensure that no unauthorized individual will have access to the personal information contained in the records prior to their destruction (e.g., locked dumpsters).

For the purposes of this statute, personal information generally includes medical information, account or credit information, account or credit application information, and tax information, by which an individual is capable of being associated through one or more identifiers.

Wisconsin law requires certain business entities to notify individuals of unauthorized acquisitions of personal information. 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.

A business that improperly disposes of such records may be required to forfeit up to $1,000 per violation and may be held liable for damages to the individual whose personal information was disposed of improperly. A person who uses personal information that was improperly disposed of is also liable for damages and may be fined not more than $1,000, imprisoned for not more than 90 days, or both. Such a violation is commonly referred to as "dumpster diving." [s. 134.97, Stats.]

NOTIFICATION REQUIREMENTS

Specified entities must provide notification regarding the unauthorized acquisition of personal information. The law applies to entities that:

- Conduct business in Wisconsin and maintain personal information in the course of business.
- License personal information in Wisconsin.
- Maintain a depository account for a Wisconsin resident.
- Lend money to a resident of Wisconsin.

An "entity" also includes:

- 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.
- A city, village, town, or county.

For purposes of the notification requirements, "personal information" means an individual's last name and 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:

- The individual's SSN.
- The individual's driver's license number or state identification number.
- 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.
- The individual's DNA profile.
- The individual's unique biometric data, including a fingerprint, voice print, retina or iris image, or any other unique physical characteristic.

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.

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.

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 if: (1) the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information; or (2) the personal information was acquired in good faith by an employee or agent of the entity and the personal information is used for a lawful purpose. [s. 134.98, Stats.]

TIMING AND METHOD OF NOTICE

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. Notice must be provided 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, the entity that provided the notice must identify the personal information that was acquired. [s. 134.98 (3), Stats.]

EXEMPTIONS

These notice provisions do not apply to financial institutions that are subject to and in compliance with federal law relating to disclosure of nonpublic personal information or to 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.

In addition, 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 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. [s. 134.98 (3m), Stats.]

RESTRICTIONS ON RECORDING OF SOCIAL SECURITY NUMBERS BY REGISTER OF DEEDS

Section 59.43 (1m), Stats., seeks to prevent individuals' SSNs 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 SSN or may remove or obscure the number; and (2) the drafter of a document that unlawfully includes an individual's SSN may be held liable for damages that the individual suffers because of the inclusion of the number.

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 SSN. Because statutes prohibit 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 the law – 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

Section 59.43 (1m), Stats., also 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

These provisions 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

Section 100.54, Stats., allows individuals to "freeze" their credit reports (referred to as "consumer reports" in the relevant federal and Wisconsin statutes and in this Information Memorandum). If an individual places a "security freeze" on his or her consumer report, then the consumer reporting agency ("CRA") may not release the consumer report to a potential creditor unless the individual has first "thawed" his or her report, thus allowing the CRA 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.

PLACING A SECURITY FREEZE

Section 100.54, Stats., provides that an individual may place a security freeze on his or her consumer report by mailing the request via certified mail to the 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.

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 statute: 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 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.

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 statutes provide 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

CRAs, as defined in the federal Fair Credit Reporting Act, must comply with the requirements of s. 100.54, Stats. However, certain entities that otherwise may be CRAs under the federal law are exempt from the statute 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.

EXCEPTIONS

The statute 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:

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, s. 100.54, Stats., requires that it also provide the individual with a notice about the Wisconsin security freeze provisions. Required notice language is included in the statutes. [See s. 100.54 (1), Stats.] 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 law is liable for actual damages sustained by an individual as a result of the failure, the costs of the action, and reasonable attorney fees.

This memorandum is not a policy statement of the Joint Legislative Council or its staff.

This memorandum was prepared by Dan Schmidt, Senior Analyst, on September 23, 2013.