

**2005 DRAFTING REQUEST**

**Assembly Amendment (AA-ASA(LRBs0512/2)-SB164)**

Received: 02/09/2006

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Jeff Fitzgerald (608) 266-2540

By/Representing: Jim Bender

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - other

Extra Copies:

Submit via email: YES

Requester's email: Rep.Fitzgerald@legis.state.wi.us

Carbon copy (CC:) to:

---

**Pre Topic:**

No specific pre topic given

---

**Topic:**

Require notification of credit bureau of unauthorized access to personal information pertaining to more than 1,000 individuals

---

**Instructions:**

See Attached

---

**Drafting History:**

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	csundber 02/13/2006	jdye 02/13/2006		_____			
/1			pgreensl 02/13/2006	_____	sbasford 02/13/2006	sbasford 02/13/2006	

FE Sent For:

<END>

**2005 DRAFTING REQUEST**

**Assembly Amendment (AA-ASA(LRBs0512/2)-SB164)**

Received: 02/09/2006

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Jeff Fitzgerald (608) 266-2540**

By/Representing: **Jim Bender**

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - other**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Fitzgerald@legis.state.wi.us**

Carbon copy (CC:) to:

---

**Pre Topic:**

No specific pre topic given

---

**Topic:**

Require notification of credit bureau of unauthorized access to personal information pertaining to more than 1,000 individuals

---

**Instructions:**

See Attached

---

**Drafting History:**

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	csundber	1 2/13 jld	2/13 PS	2/13 selb			

FE Sent For:

<END>

2/3/06 Jim Bender / Jeff Fitzgerald

Simple amend to ASA to SSA 3 to SB 164:

require notification of credit bureau if  
unauthorized access to PI pertaining to  
more than 1,000 individuals

Proposed Amendments to Wisconsin S.B. 164, Third Substitute

Page 5, line 11.

1

After "personal information.", insert the following:

NO CONTACT → THEN

"(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

Explanation

When a business sends to consumers a notice of a breach, it will often direct those consumers to contact a consumer reporting agency, who will then be entitled to a credit report for free since those consumers are potential fraud victims. If Acme Bank is sending out 100,000 breach notices, consumer reporting agencies must be prepared to handle those consumers. Advance notice to consumer reporting agencies of breach notice distribution allows those agencies to be fully prepared to adequately serve the consumer. This may mean adding additional personnel to staff telephones, open mail, operate computers, and similar processes. Further, if the breach is sizable, than a consumer reporting agency may want to open a dedicated phone line to serve the needs consumers affected by that breach. Prompt attention to consumers by consumer reporting agencies just good consumer service, it is required by the federal Fair Credit Reporting Act (FCRA).

Page 6, line 14.

After "this subsection.", insert the following:

2

"(8m) In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices."

Separate Amend.  
1,000

Explanation

Security breach legislation must make an adequate distinction between data owners and third party entities that merely process data on behalf of a data owner. This is the approach taken in California, the first security breach law in the nation, and all other state security breach laws that have followed. Many companies need this distinction because they do not have a direct relationship with a consumer and it is far more appropriate for businesses and their customers if the business that owned the data provided the notification to its own customer, rather than some company the consumer has never head of before. From an operational perspective, a data processor may not always have sufficient contact information to contact the consumer. For example, a credit card processor may only have the credit or debit card number of the consumer and that consumer's name. Rarely will such a data processor have an address as well. Similarly, a check processor may have bank account, routing and check numbers, as well as the amount of the check at issue, but the processor may not have the consumer's address.

Consumers and businesses are better served if the data owner contacted the consumer directly and not a third party data processor. This is the approach taken by current practices and federal guidelines. The Visa/MasterCard Association rules require that payment processors notify the financial institution if a data processor has a breach. The federal interagency guidelines for security breach notification directs service providers to notify financial institutions so that those institutions may notify their customers in the manner that is best to meet the needs of the financial institution/customer relationship. 70 Fed. Reg. 15736 (March 29, 2005) (Interagency Guidance [FTC, OTS, FRB, FDIC] on Response Programs for Unauthorized Access to Customer Information and Customer Notice).

Finally, the issue was well summarized in testimony from Carlos Minetti (from Discover credit card services) during the July 21 before the House Financial Services Committee hearing on data processors.

in the event of a data breach affecting credit card information, notification is best handled by the card issuer, not the entity whose security was breached. That entity whose security was compromised must cooperate fully in providing the details necessary to ensure efficient response and notification by the issuer, and to prevent further fraud. But requiring merchants or processors to directly notify affected cardholders may impose an obligation that they cannot readily achieve (since they may not have the necessary consumer contact information), and can needlessly alarm individuals who were not adversely affected by the breach. This might encourage consumers to take steps that are unnecessary (e.g., closing accounts, placing fraud alerts on credit reports). A single notice is the best way to protect credit card users, and card issuers are in the best position to determine whether and when that notice is appropriate.

**ASSEMBLY SUBSTITUTE AMENDMENT ,  
TO 2005 SENATE BILL 164**

1     **AN ACT** *to create* 895.507 of the statutes; **relating to:** notice regarding  
2     unauthorized acquisition of personal information.

---

***Analysis by the Legislative Reference Bureau***

This substitute amendment requires an entity that possesses certain personal information about an individual to notify the individual when the information is acquired by a person who the entity has not authorized to do so (unauthorized acquisition). The substitute amendment's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; license personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident.

Under the substitute amendment, personal information includes any of the following information about an individual, if combined with the name of the individual to whom the information pertains: driver's license number; social security number; financial account number and certain related information; and deoxyribonucleic acid (DNA) profile and other biometric data. Personal information does not include information that is lawfully available to the public or information that is encrypted.

As to an entity whose principal place of business is located in Wisconsin or that licenses personal information in Wisconsin, if the entity knows or has reason to know of an unauthorized acquisition, the substitute amendment requires the entity to

make reasonable efforts to notify the individual that is the subject of the personal information (subject) that the individual's personal information has been acquired. As to an entity whose principal place of business is not located in Wisconsin, if the entity knows or has reason to know of an unauthorized acquisition involving information pertaining to a Wisconsin resident, the substitute amendment requires the entity to make reasonable efforts to notify the subject. An entity is not required to give notice if the acquisition of personal information does not create a material risk of identity theft or fraud, or if the personal information was acquired in good faith by an employee of the entity and the personal information is used for a lawful purpose of the entity.

Under the substitute amendment, an entity required to notify a subject must, within a reasonable time not to exceed 45 days after learning of the unauthorized acquisition, inform the subject that the entity knows of the unauthorized use of personal information pertaining to the subject. The entity must deliver the notice by mail or by another method the entity has previously used to communicate with the subject. If the entity cannot reasonably determine the subject's mailing address, the entity may notify the subject by another means reasonably calculated to provide actual notice to the subject. Upon request by a person who receives a notice, an entity must identify the personal information that was acquired.

Under the substitute amendment, a separate notification requirement applies to a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information. The requirement only applies if there is no contract between the person that stores the personal information and the person that owns or licenses the personal information. If such a person knows that personal information in the person's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must notify the person that owns or licenses the personal information as soon as practicable.

Under the substitute amendment, a law enforcement agency may request an entity to delay a required notice for any period of time in order to protect an investigation or homeland security. An entity that receives such a request must begin the notification process after the requested delay period.

The substitute amendment contains exemptions from the notice requirements for certain entities that are subject to, and in compliance with, certain requirements imposed by federal law and regulations that generally relate to the privacy and security of medical and financial data. The substitute amendment also prohibits the enactment or enforcement by a city, village, town, or county of an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

The substitute amendment provides that failure to comply with the substitute amendment's requirements is not negligence or a breach of a legal duty, but may be evidence of negligence or a breach of a legal duty.

---

*The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:*

1           SECTION 1. 895.507 of the statutes is created to read:

2           **895.507 Notice of unauthorized acquisition of personal information.**

3           (1) DEFINITIONS. In this section:

4           (a) 1. "Entity" means a person, other than an individual, that does any of the  
5 following:

6           a. Conducts business in this state and maintains personal information in the  
7 ordinary course of business.

8           b. Licenses personal information in this state.

9           c. Maintains for a resident of this state a depository account as defined in s.  
10 815.18 (2) (e).

11           d. Lends money to a resident of this state.

12           2. "Entity" includes all of the following:

13           a. The state and any office, department, independent agency, authority,  
14 institution, association, society, or other body in state government created or  
15 authorized to be created by the constitution or any law, including the legislature and  
16 the courts.

17           b. A city, village, town, or county.

18           (am) "Name" means an individual's last name combined with the individual's  
19 first name or first initial.

1 (b) “Personal information” means an individual’s last name and the  
2 individual’s first name or first initial, in combination with and linked to any of the  
3 following elements, if the element is not publicly available information and is not  
4 encrypted, redacted, or altered in a manner that renders the element unreadable:

5 1. The individual’s social security number.

6 2. The individual’s driver’s license number or state identification number.

7 3. The number of the individual’s financial account number, including a credit  
8 or debit card account number, or any security code, access code, or password that  
9 would permit access to the individual’s financial account.

10 4. The individual’s deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).

11 5. The individual’s unique biometric data, including fingerprint, voice print,  
12 retina or iris image, or any other unique physical representation.

13 (c) “Publicly available information” means any information that an entity  
14 reasonably believes is one of the following:

15 1. Lawfully made widely available through any media.

16 2. Lawfully made available to the general public from federal, state, or local  
17 government records or disclosures to the general public that are required to be made  
18 by federal, state, or local law.

19 **(2) NOTICE REQUIRED.** (a) If an entity whose principal place of business is  
20 located in this state or an entity that maintains or licenses personal information in  
21 this state knows that personal information in the entity’s possession has been  
22 acquired by a person whom the entity has not authorized to acquire the personal  
23 information, the entity shall make reasonable efforts to notify each subject of the  
24 personal information. The notice shall indicate that the entity knows of the

1 unauthorized acquisition of personal information pertaining to the subject of the  
2 personal information.

3 (b) If an entity whose principal place of business is not located in this state  
4 knows that personal information pertaining to a resident of this state has been  
5 acquired by a person whom the entity has not authorized to acquire the personal  
6 information, the entity shall make reasonable efforts to notify each resident of this  
7 state who is the subject of the personal information. The notice shall indicate that  
8 the entity knows of the unauthorized acquisition of personal information pertaining  
9 to the resident of this state who is the subject of the personal information.

10 (bm) If a person, other than an individual, that stores personal information  
11 pertaining to a resident of this state, but does not own or license the personal  
12 information, knows that the personal information has been acquired by a person  
13 whom the person storing the personal information has not authorized to acquire the  
14 personal information, and the person storing the personal information has not  
15 entered into a contract with the person that owns or licenses the personal  
16 information, the person storing the personal information shall notify the person that  
17 owns or licenses the personal information of the acquisition as soon as practicable.

18 (cm) Notwithstanding pars. (a), (b),  [and (bm)] an entity is not required to  
19 provide notice of the acquisition of personal information if any of the following  
20 applies:

21 1. The acquisition of personal information does not create a material risk of  
22 identity theft or fraud to the subject of the personal information.

23 2. The personal information was acquired in good faith by an employee or agent  
24 of the entity, if the personal information is used for a lawful purpose of the entity.

1           **(3) TIMING AND MANNER OF NOTICE; OTHER REQUIREMENTS.** (a) Subject to sub. (5),  
2 an entity shall provide the notice required under sub. (2) within a reasonable time,  
3 not to exceed 45 days after the entity learns of the acquisition of personal  
4 information. A determination as to reasonableness under this paragraph shall  
5 include consideration of the number of notices that an entity must provide and the  
6 methods of communication available to the entity.

7           (b) An entity shall provide the notice required under sub. (2) by mail or by a  
8 method the entity has previously employed to communicate with the subject of the  
9 personal information. If an entity cannot with reasonable diligence determine the  
10 mailing address of the subject of the personal information, and if the entity has not  
11 previously communicated with the subject of the personal information, the entity  
12 shall provide notice by a method reasonably calculated to provide actual notice to the  
13 subject of the personal information.

14           (c) Upon written request by a person who has received a notice under sub. (2),  
15 the entity that provided the notice shall identify the personal information that was  
16 acquired.

17           **(3m) REGULATED ENTITIES EXEMPT.** This section does not apply to any of the  
18 following:

19           (a) An entity that is subject to, and in compliance with, the privacy and security  
20 requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation  
21 to such an entity, if the entity or person has in effect a policy concerning breaches of  
22 information security.

23           (b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with  
24 the requirements of 45 CFR part 164.





State of Wisconsin  
2005 - 2006 LEGISLATURE

LRBa2297/1 RWR

CTS: ^...

W: 2/12/06

Wanted: Tues. AM

Jed

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

ASSEMBLY AMENDMENT,

TO ASSEMBLY SUBSTITUTE AMENDMENT (LRBs0512/2),

TO 2005 SENATE BILL 164

DN

1 At the locations indicated, amend the substitute amendment as follows:

2 1. Page 5, line 9: after that line insert:

3 "(br) If, as the result of a single incident, an entity is required under par. (a) or  
4 (b) to notify 1,000 or more individuals that personal information pertaining to the  
5 individuals has been acquired, the entity shall without unreasonable delay notify all  
6 consumer reporting agencies that compile and maintain files on consumers on a  
7 nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and  
8 content of the notices sent to the individuals."

9 2. Page 5, line 18: delete "and (bm)" and substitute "(bm), and (br)".

10 3. Page 6, line 14: delete "(2)" and substitute "(2) (a) or (b)".

11 (END)

**DRAFTER'S NOTE**  
**FROM THE**  
**LEGISLATIVE REFERENCE BUREAU**

LRBa2297/1dn

CTS: ^:....

JLD

Rep. Fitzgerald:

✓ This amendment adds a requirement to notify credit reporting agencies under certain circumstances. Please review this draft carefully to ensure it is consistent with your intent.

Note that the drafting instructions indicate that the required notice should advise credit reporting agencies of the timing, distribution, and content of the notices sent to individuals. It is not clear what information would be included in a notice of timing, distribution, and content. Should the amendment be more specific? For example, the amendment could require that a notice to credit reporting agencies specify when the unauthorized acquisitions occurred, when the entity learned of the unauthorized acquisitions, when the entity provided notice to affected individuals, how the entity provided such notice, how many individuals were notified, etc.

↖ and

Christopher T. Sundberg  
Legislative Attorney  
Phone: (608) 266-9739  
E-mail: christopher.sundberg@legis.state.wi.us

**DRAFTER'S NOTE  
FROM THE  
LEGISLATIVE REFERENCE BUREAU**

LRBa2297/1dn  
CTS:jld:pg

February 13, 2006

Rep. Fitzgerald:

This amendment adds a requirement to notify credit reporting agencies under certain circumstances. Please review this draft carefully to ensure it is consistent with your intent.

Note that the drafting instructions indicate that the required notice should advise credit reporting agencies of the timing, distribution, and content of the notices sent to individuals. It is not clear what information would be included in a notice of timing, distribution, and content. Should the amendment be more specific? For example, the amendment could require that a notice to credit reporting agencies specify when the unauthorized acquisitions occurred, when the entity learned of the unauthorized acquisitions, when the entity provided notice to affected individuals, how the entity provided such notice, and how many individuals were notified, etc.

Christopher T. Sundberg  
Legislative Attorney  
Phone: (608) 266-9739  
E-mail: christopher.sundberg@legis.state.wi.us