



State Security Breach Legislation

February 2006

Doug Markiewicz, CISSP



Table of Contents

1	Introduction	2
2	Scope	3
3	Existing Legislation	4
3.1	Definition of Personal Information	4
3.2	Notification Requirements	5
3.3	Notification Procedures	5
3.4	Notification Timelines.....	6
3.5	Other Provisions	7
3.5.1	Safeguarding Personal Information.....	7
3.5.2	Data Destruction and Disposal.....	7
3.5.3	Security Freezes.....	7
4	Common Deviations in Current Legislation	8
4.1	Defining Personal Information	8
4.2	Encryption	8
4.3	Notification Timelines.....	8
4.4	Determining No-Risk Security Breach.....	9
5	Recommendations	10
	Appendix A – State Law Effective Date Table	11
	Appendix B – State Notification Procedures Table	12
	Appendix C – State Legislation Reference	13



1 Introduction

In August 2002, California passed ground-breaking identity theft legislation that requires a person, business or government agency to disclose any security breach that involves the compromise of personal information of a state resident. This legislation, commonly referred to as California Senate Bill 1386¹, was the first state or federal law to specifically require disclosure of a security breach. S.B. 1386 cited a 108% increase in identity theft cases at the Los Angeles County Sheriff's Department in 2000.² A 2003 survey conducted by the Federal Trade Commission suggested that 3.25 million Americans had discovered misuse of their personal information in the previous 12 months, with an average cost for the victim at \$4,800. This same study found that the cost of an incident of identity theft is significantly smaller if the misuse of the victim's personal information is discovered quickly.³

On February 15, 2005, ChoicePoint announced that personal information of 145,000 customers had been compromised by identity thieves who registered fake accounts with the company. This was the first in a long list of public disclosures that occurred throughout 2005. This incident was quickly followed by security breach disclosures from Bank of America, DSW Retail Ventures and LexisNexis. The Privacy Rights Clearinghouse documented 100 security breaches that impacted over 52 million customers since the ChoicePoint incident.⁴ Security breaches were not limited to commercial entities either. Academic institutions, health care facilities and government agencies were impacted as well. Approximately half (48%) of the 100 security breaches documented by the Privacy Rights Clearinghouse in 2005 were of academic institutions, though over 90% of the 52 million customers were impacted as a result of breaches in the commercial sector.

As a result, many states began passing identity theft legislation that required public disclosure of security breach information. As of the publication date of this white paper, 23 states have enacted legislation (See Appendix A) and another 12 states have bills before state Congress. Most states used California S.B. 1386 as a model for their own legislation. However, each state's legislation is ultimately unique.

This white paper analyzes existing state identity theft legislation, discusses their gaps and provides recommendations for improvement. Finally, this paper makes recommendations on how a covered entity can best cope with the range of identity theft bills.

¹ California Senate Bill 1386 was implemented in California Civil Code Section 1798.29. The bill number, however, is more commonly recognized throughout industry and will therefore be used in this document.

² [California Senate Bill 1386](#). (2002)

³ Federal Trade Commission. Identity Theft Survey Report. September 2003.
<http://www.ftc.gov/os/2003/09/synovaterreport.pdf>

⁴ A Chronology of Data Breaches Reported Since the ChoicePoint Incident. Privacy Rights Clearinghouse.
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>.



2 Scope

This white paper discusses state identity theft legislation that requires disclosure of security breaches. Specifically, it analyzes consumer notification requirements, procedures and exemptions and any pertinent terminology. Discussion of penalties associated with non-compliance is out of the scope of this document. While this paper discusses legal issues and requirements, it should not be construed or used as legal guidance.



3 Existing Legislation

The California legislature passed Senate Bill 1386 in August 2002. No state passed similar legislation until 2005. Today, all but 15 states have either passed legislation or have bills before state Congress requiring disclosure of security breaches. Virtually all states have used California S.B. 1386 as a baseline for developing their individual bills. The following sections explain various components of California's bill and compare it to bills passed by other states.

3.1 Definition of Personal Information

The term *personal information* or *personally identifiable information (PII)* is used when describing the type of data compromise that requires disclosure to customers. California law defines a security breach as "...unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information..." Thus the definition of personal information becomes important. Section 1798.82e of California Civil Code defines personal information as follows:

1798.82(e) - For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

There are several key points to this definition. A social security number alone does not constitute personal information. Only when it is coupled with the individual's name does it become personal information. Also, California defines personal information as an unencrypted data format. This presents an issue due to the fact that the bill does not properly define what constitutes encryption. This issue is discussed in greater detail in Section 4.

Of the 23 states that have passed legislation, 16 have adopted a definition of personal information similar to that of California. Several states have expanded upon this definition to include other types of information including medical information, account passwords, date of birth, mother's maiden name, etc. Definitions adopted by North Dakota and North Carolina exhibit the greatest expansion in defining personal information. They include the following:

North Dakota

- The operator's license number assigned to an individual by the Department of Transportation
- A non-driver color photo identification card number assigned to the individual by the Department of Transportation under section 39-06-03.1
- The individual's date of birth
- The maiden name of the individual's mother
- An identification number assigned to the individual by the individual's employer
- The individual's digitized or other electronic signature

North Carolina

- Electronic identification numbers
- Digital signatures
- Biometric data
- Fingerprints

- Passwords
- Parent's legal surname prior to marriage

States with pending legislation have followed the trend by adopting California's definition of personal information. An interesting exception to this trend is in Arizona where personal information is already defined in [Arizona Statute 13-2001\(10\)](#).

13-2001(10) - Personal identifying information means any written document or electronic data that does or purports to provide information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number, photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information.

Included in this definition are a number of unique pieces of information including screen names, email signatures, DNA and genetic information. Several bills currently before Arizona's House employ this definition.

3.2 Notification Requirements

Most states have also taken a lead from California when defining the requirements of their disclosure laws. California law states the following:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

1798.82 (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.

California makes a distinction between an entity that owns or licenses data and an entity that maintains data. The responsibility of notifying customers following a security breach is placed solely in the hands of an entity that owns or licenses data. California also includes the same clauses for government agencies. The term *unencrypted personal information* is used to describe the type of data that requires notification. However, as mentioned previously, the law does not identify what constitutes encryption of personal information. These requirements also leave room for interpretation in the phrase "...reasonably believes to have been, acquired by an unauthorized person." These points are discussed in later sections.

A number of states have added exceptions to the notification requirements. Multiple states have included a clause stating that notification is not required if, after a reasonable investigation, an entity determines there is no reasonable likelihood of harm to the consumer. No further framework is provided for assisting in making this determination. Several states have also included provisions that exclude financial institutions that are bound to related requirements of the [Gramm-Leach Bliley Act](#).

3.3 Notification Procedures

Notification procedures are clearly defined in the state security breach laws. They define specific methods of notification and what content is required within the text of the notification. Notice in California consists of one of the following three methods:



- 1) Written notice
- 2) Electronic notice
- 3) Substitute notice.

Electronic notification must be consistent with the Electronic Signatures in Global and National Commerce Act ([15 U.S.C. 7001](#)), which states that a consumer must consent to receipt of electronic notice.

Substitute notice was developed to handle large security breaches. In California, substitute notice can be used if the cost to provide written or electronic notice exceeds \$250,000 or if more than 500,000 consumers are impacted. Substitute notice consists of all of the following:

- 1) Email notice if an email address is on file
- 2) Conspicuous posting on the entity's website
- 3) Notification of major state-wide media.

The difference between electronic notice as a primary form of notification and email notice as a substitute form of notification is that email notice does not require consent from the consumer - it is merely a good faith attempt at providing email notification.

Other states followed trends in establishing notification requirements. Several states added the option of telephone notice as a primary form of notification. Several states also modified the terms in which substitute notice can be used. For example, in Delaware, substitute notice can be leveraged if the cost of the primary forms of notification exceeds \$75,000 or if the number of impacted consumers exceeds 100,000. Maine chose to use \$5,000 or 1,000 consumers as their criteria for substitute notice. In all, 17 states adopted the same notification requirements as the state of California. Appendix B provides a state-by-state analysis of notification requirements.

One popular requirement that California did not include as part of S.B. 1386 was notification to consumer reporting agencies. 15 states include provisions stating that if a specified number of consumers are notified of a security breach then consumer reporting agencies must also be notified. The term *consumer reporting agencies* is defined in section 603 of the [Fair Credit Reporting Act \(15 U.S.C. 1681a\)](#) as

"...any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

The terms of notification vary from state to state. Minnesota specifies that consumer reporting agencies must be notified if more than 500 consumers are informed of a breach of their personal information, while Georgia and Texas require such notification if more than 10,000 consumers are informed. Montana requires that consumer reporting agencies be notified of all security breaches that require notification to consumers. Appendix B provides a state-by-state analysis of requirements for sending notification to consumer reporting agencies.

3.4 Notification Timelines

The timeline for sending notification to consumers is vague in most state legislation. [California Civil Code Section 1789.29\(a\)](#) states, "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement...or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." This leaves substantial room for interpretation by the covered entity. We will discuss this further in the next section when we take a look at gaps in existing state laws. Most states have adopted some iteration of this time requirement, with the exception of Florida and Ohio where notification must be made within 45 days of the security breach.

Most states include a provision stating that notification can be delayed if such notification would impede a criminal investigation. This determination must be made by law enforcement officials. North Carolina and Ohio add that notification can be delayed if it would jeopardize national security.

3.5 Other Provisions

Several states have made an attempt to develop a more comprehensive identity theft bill that includes more than just disclosure of security breaches. Some states include requirements to safeguard personal information while others include requirements for secure data destruction and disposal. Several states also include a provision allowing consumers to place a freeze on their credit report after being subjected to identity theft.

3.5.1 Safeguarding Personal Information

Arkansas, Nevada and Texas include provisions for the implementation of security processes and procedures. [Texas Code Title 4 Chapter 48.102](#) states, "A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information..." This provision is important because it places accountability on a covered entity to actually protect personal information. Arkansas and Nevada provisions contain the same requirement with slight variations in wording.

3.5.2 Data Destruction and Disposal

A number of states (Arkansas, Montana, Nevada, New Jersey, North Carolina and Texas) have passed provisions related to destruction and disposal of personal information. While not worded identically, these provisions all state that an entity must destroy or arrange for the destruction of customer records containing personal information if the records are no longer needed for business purposes. Montana, New Jersey and Texas specify that destruction must be conducted through shredding, erasing or otherwise modifying records to make them unreadable and undecipherable.

North Carolina expands significantly upon data destruction provisions. Their requirements call for implementation of policies and procedures as well as a program for monitoring compliance with these policies and procedures. If an entity chooses to leverage a third party service provider, North Carolina requires an audit of the third party's operational procedures and review of its information security policies and procedures. The third-party service provider must also be certified by a recognized trade association.

3.5.3 Security Freezes

Connecticut, New Jersey and North Carolina have included provisions that allow a consumer to place a freeze on their credit report if they've been notified of a security breach impacting their personal information. The security freeze provisions typically require a consumer to submit a security freeze request to credit reporting agencies and, upon enactment of the security freeze, all requests for release of credit information to a third party must first be authorized by the consumer. These provisions also allow consumer reporting agencies to charge a fee for these services. In Connecticut, these fees are specified as no more than \$10 for adding or removing a security freeze and \$12 for temporarily lifting a security freeze. New Jersey requires no fee when initiating a security freeze, and a maximum of \$5 for temporarily lifting a security freeze. North Carolina sets a maximum of \$10 for all activities.

4 Issues in Current Legislation

A number of deviations exist in current state identity theft laws regarding security breach notification. While several of these issues have been mentioned briefly in previous sections, this section provides a more detailed discussion of these deviations, and the following section identifies recommended actions for the future.

4.1 Defining Personal Information

Defining personal information is one of the most difficult issues associated with security breach and identity theft law. Many existing state laws do not provide a complete definition of personal information. Several states have taken a step in the right direction by expanding upon the wording in California S.B. 1386. Most state laws only cover social security numbers, state issued ids, and financial account information that is coupled with a first and last name. Under this definition, a social security number coupled with an address and phone number would not constitute personal information despite the fact that a name could be determined with basic social engineering tactics. Even without the first and last name requirement, most state laws fall short of adequately defining personal information. State legislatures must define a comprehensive definition of personal information that includes personal information such as medical records, non-financial account IDs and passwords, and biometric data.

4.2 Encryption

Vague language in encryption requirements weakens current security breach laws. Such vagueness leads to the question of whether or not compromise of encrypted personal information constitutes a security breach. As mentioned previously, California defines a security breach as unauthorized access to personal information, and then specifically defines personal information as being unencrypted. In this context, the security of encrypted information is dependent upon the strength of the cipher used for encryption and how well the encryption keys are protected.

The second issue - the lack of a clear definition of encryption – is more widespread. The lack of a proper definition of encryption allows leeway for entities to decide what definition might best suit a particular situation. These definitions may be influenced by political and financial issues and may not be representative of industry best practice.

Several states (Maine, Nevada, North Carolina, Ohio and Pennsylvania) have attempted to define encryption. Maine defines encryption as, “Disguising of data using generally accepted practices.”⁵ No further clarification is given on what constitutes generally accepted practices. North Carolina, Ohio and Pennsylvania define encryption as, “The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.”⁶ This is a fairly solid definition but lacks clarity in terms of what actual cipher suites should be leveraged.

4.3 Notification Timelines

Notification requirements are vague in state security breach laws, with the exception of Florida and Ohio. In most cases, notification must be made “...in the most expedient time possible and without unreasonable delay...”⁷ Unreasonable is a subjective term and will likely vary depending

⁵ Maine R.S. Title 10 Chapter 210-B Section 1347(2). <http://janus.state.me.us/legis/statutes/10/title10ch210-B.pdf>.

⁶ Pennsylvania Act 2005-94. <http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf>.

⁷ Common language used in numerous state laws. Originated in [California Senate Bill 1386](#).



on the circumstances of each covered entity. In June 2005, the personal information of 40 million consumers was compromised when CardSystems was breached. Notification could take months if CardSystems elects to not use substitute notice with that many consumers. This poses the question of whether a customer should have to wait months to find out that their personal information has been compromised.

Another topic that requires further exploration is whether or not notification should be delayed long enough "...to determine the scope of the breach and restore the reasonable integrity of the data system."⁸ Determining the scope of a security breach and restoring the integrity of a system may require a significant amount of time and effort. Upon discovery of a security breach, an incident response plan is initiated and a forensic investigation can be conducted. Depending on the scope and severity of the breach, a forensic investigation can be very costly and time consuming. In February 2005, ChoicePoint disclosed a security breach impacting 145,000 consumers and it wasn't until September 2005 that the determination was made that almost 10,000 additional consumers were impacted. This example illustrates the time it can take to conduct an investigation and determine the scope of a security breach. 10,000 consumers were not notified of a breach in their personal information until 7 months after the breach. State security breach laws need to clearly define what constitutes a reasonable delay of notification and hold states accountable if these requirements are not met. Florida and Ohio accomplish this by stating notification is required within 45 days.

4.4 Determining No-Risk Security Breach

Several states include clauses that specify that a covered entity is not required to notify consumers if the covered entity determines there is no "reasonable likelihood of harm" to the consumer after a "reasonable investigation". Arkansas, Connecticut, Florida, Louisiana, New Jersey and Rhode Island have all passed provisions of this nature. Much like the previous discussion of reasonable delay, the definition of a reasonable investigation or the reasonable likelihood of harm is left open for interpretation. No state or federal framework currently exists for making this type of determination. Some of these states require that the investigation is performed with the help of law enforcement, which adds more credibility to making the determination. However, without a framework, the determination will vary depending on the entity conducting the investigation.

⁸ Common language used in numerous state laws. Originated in [California Senate Bill 1386](#).

5 Recommendations

A number of steps can be taken to improve existing state legislation. States should expand upon existing definitions for personal information, and these definitions should not be defined strictly as unencrypted data. Arizona and North Carolina have the most thorough definitions of personal information. Security breach laws should target all forms of personal information, as breaches don't solely target unencrypted information. Standards should define whether or not a particular encryption control provides an acceptable level of protection for personal information. States should reference existing standards or call for the development of new standards to define acceptable security controls and ensure a consistent application of legal requirements. The National Institute of Standards and Technology (NIST) and the Institute of Electrical and Electronics Engineers (IEEE) both develop standards related to encryption. The IEEE Security in Storage Working Group will soon be publishing standards for encryption of stored data and states should consider requiring compliance with these standards.

States also need to eliminate subjective requirements that leave room for individual interpretation. For example, Florida and Ohio specify a 45-day notification requirement for security breaches, whereas other states do not specify a timeframe. States should also call for the development of comprehensive frameworks that clarify issues such as the timeframes of notification and determining a no-risk security breach.

For covered entities looking to integrate security breach disclosure law requirements, a concise set of policies and accompanying procedures is necessary. The following four steps will not only assist in efforts to comply with state laws, but will enhance overall information security and privacy practices for a covered entity:

1. Develop a comprehensive security program to protect the confidentiality, integrity and availability of all information, not just personal information. Reference existing standards such as ISO 17799 in creating this security program.
2. Develop data classification standards that identify personally identifiable information while taking into consideration existing legislation. Arizona, North Carolina and North Dakota provide the most encompassing definitions of personally identifiable information and would provide the best starting point for internal policies.
3. Conduct a risk assessment of all personally identifiable information to ensure that proper security controls (i.e. authentication and encryption) are in place to protect these information assets. When implementing security controls, reference existing industry standards, such as those published by the Federal Trade Commission, NIST and IEEE. NIST specifically addresses encryption controls in the Federal Information Processing Standards, which define acceptable cipher suites, and the IEEE Security and Storage Working Group will soon be publishing standards for the protection of data at rest.
4. Develop a policy for handling security breaches that addresses the compromise of personally identifiable information. This policy should take into consideration all state laws. Consulting a legal adviser will help ensure that a policy is comprehensive and encompasses the requirements of relevant states.

It is expected that the federal government will pass its own identity theft legislation in 2006 that includes security breach disclosure requirements. Several bills are currently before Congress with backing from influential senators (See S.1789 and S.1408). These federal bills place more requirements on covered entities than existing state laws. Acting now will ensure proper preparation for future legislation.

Appendix A – State Law Effective Date Table

State	Signed	Effective
Arkansas	April 4, 2005	April 4, 2005
California	August 30, 2002	July 01, 2003
Connecticut	June 24, 2005	January 1, 2006
Delaware	June 28, 2005	September 6, 2005
Florida	June 14, 2005	July 1, 2005
Georgia	June 5, 2005	June 5, 2005
Illinois	June 16, 2005	January 1, 2006
Indiana	April 26, 2005	July 1, 2006
Louisiana	July 12, 2005	January 1, 2006
Maine	June 10, 2005	January 31, 2006
Minnesota	June 2, 2005	January 1, 2006
Montana	April 28, 2005	March 1, 2006
Nevada	June 17, 2005	January 1, 2006
New Jersey	September 22, 2005	March 21, 2006
New York	August 9, 2005	December 7, 2005
North Carolina	September 21, 2005	December 1, 2005
North Dakota	April 22, 2005	June 1, 2005
Ohio	November 17, 2005	February 17, 2006
Pennsylvania	December 22, 2005	June 20, 2006
Rhode Island	July 10, 2005	March 01, 2006
Tennessee	June 18, 2005	July 1, 2005
Texas	June 17, 2005	September 1, 2005
Washington	May 10, 2005	July 24, 2005

Indicates a state with an effective date in the future.



Appendix B – State Notification Procedures Table

State	Written Notice	Electronic Notice	Telephone Notice	Consumer Credit Notice	Substitute Notice		
					Affected Class	Cost Requirements	Affected Class
Arkansas	x	x			\$250,000	500,000	E, M, W
California	x	x			\$250,000	500,000	E, M, W
Connecticut	x	x	x		\$250,000	500,000	E, M, W
Delaware	x	x	x		\$75,000	100,000	E, M, W
Florida	x	x		1,000	\$250,000	500,000	E, M, W
Georgia	x	x		10,000	\$250,000	500,000	E, M, W
Illinois	x	x			\$250,000	500,000	E, M, W
Indiana	x	x		1,000	\$250,000	500,000	M,W
Louisiana	x	x			\$250,000	500,000	E, M, W
Maine	x	x		1,000	\$5,000	1,000	E, M, W
Minnesota	x	x		500	\$250,000	500,000	E, M, W
Montana	x	x	x	All	\$250,000	500,000	E, M, W
Nevada	x	x		1,000	\$250,000	500,000	E, M, W
New Jersey	x	x		1,000	\$250,000	500,000	E, M, W
New York	x	x	x	5,000	\$250,000	500,000	E, M, W
North Carolina	x	x	x	1,000	\$250,000	500,000	E, M, W
North Dakota	x	x			\$250,000	500,000	E, M, W
Ohio	x	x	x	1,000	\$250,000	500,000	E, M, W
Pennsylvania	x	x	x	1,000	\$100,000	175,000	E, M, W
Rhode Island	x	x		1,000	\$25,000	50,000	E, M, W
Tennessee	x	x		1,000	\$250,000	500,000	E, M, W
Texas	x	x		10,000	\$250,000	500,000	E, M, W
Washington	x	x			\$250,000	500,000	E, M, W

Key

E = Email

M = Notification via major statewide media

W = Posting of notice on the institution's website

 Indicates a deviation from California notification requirements.

Appendix C – State Legislation Reference

State	Implementing Law	Hyperlink
Arkansas	Arkansas Code Title 4 Subtitle 7 Chapter 110	http://www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf
California	California Civil Code Section 1798.29 California Civil Code Section 1798.82 and 1798.84	http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
Connecticut	Public Act 05-148	http://www.cga.ct.gov/2005/ACT/Pa/pdf/2005PA-00148-R00SB-00650-PA.pdf
Delaware	Title 6 Subtitle II Chapter 12B	http://www.delcode.state.de.us/title6/c012b/index.htm
Florida	Florida Statutes Title XLVI Chapter 817 Section 568	http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC5681.HTM&Title=-%3E2005-%3ECh0817-%3ESection%205681#0817.5681
Georgia	Georgia Code Title 10 Chapter 1 Section 910-912	http://www.legis.ga.gov/legis/2005_06/pdf/sb230.pdf
Illinois	815 ILCS 530	http://www.ilga.gov/legislation/94/HB/PDF/09400HB1633lv.pdf
Indiana	Indiana Code Title 4 Article 1 Chapter 11	http://www.in.gov/legislative/ic/code/title4/ar1/ch11.pdf
Louisiana	Louisiana Revised Statutes Chapter 51 Title 51 Section 3071-3077	http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093
Maine	Maine Revised Statute Title 10 Chapter 210-B	http://janus.state.me.us/legis/statutes/10/title10ch210-B.pdf
Minnesota	Minnesota Statute Chapter 325E.61	http://www.revisor.leg.state.mn.us/stats/325E/61.html
Montana	Montana Code Title 31 Chapter 3 Section 115	http://data.opi.state.mt.us/bills/2005/billhtml/HB0732.htm
Nevada	Nevada Revised Statutes Title 52	http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf
New Jersey	P.L. 2005 Chapter 226	http://www.njleg.state.nj.us/2004/Bills/PL05/226_.PDF
New York	Chapter 442	http://assembly.state.ny.us/leg/?bn=A04254&sh=t
North Carolina	Session Law 2005-414	http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/PDF/S1048v6.pdf
North Dakota	North Dakota Century Code Chapter 51-30	http://www.legis.nd.gov/cencode/t51c30.pdf



Ohio	Ohio Revised Code Title 13 Chapter 1347	http://www.legislature.state.oh.us/bills.cfm?ID=126_H_B_104
Pennsylvania	Act 2005-94	http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf
Rhode Island	General Law Title 11 Section 49.2	http://www.rilin.state.ri.us/PublicLaws/Law05/law05225.htm
Tennessee	Tennessee Code Title 47 Chapter 18 Part 21	http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0473.pdf
Texas	Texas Code Title 4 Chapter 48	http://www.capitol.state.tx.us/data/docmodel/79r/billtext/pdf/SB00122F.PDF
Washington	Revised Code of Washington Title 19 Chapter 255 Section 010	http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010