

Model State Clean Credit and Identity Theft Protection Act

**THE CLEAN CREDIT AND IDENTITY THEFT PROTECTION
ACT: MODEL STATE LAWS**

**THE CLEAN CREDIT AND IDENTITY THEFT PROTECTION
ACT: MODEL STATE LAW**

**Consumers Union of U.S., Inc and the state Public Interest
Research Groups**

Updated August 2007

**For more information contact the editors:
Gail Hillebrand and Michelle Jun of Consumers Union (415)431-6747
Ed Mierzwinski of U.S. PIRG (202)546-9707 x 314**

INTRODUCTION

What this model law does:

This model identity theft legislation offers consumers with protections from identity theft. This model law was first issued in 2004, and it provided a framework for state bills, particularly on security freezes and notice of data breach, throughout the country. Most of the changes in this August 2007 revision are updates to reflect key improvements that have been adopted, or considered, in state legislatures. In six sections, the model act addresses:

- Social Security Number Protection;
- Security Freeze;
- Prevention of and Protection From Security Breaches;
- Right to File a Police Report Regarding Identity Theft;
- Adequate Destruction of Personal Records; and
- Severability Clause.

SECTION 1: SOCIAL SECURITY NUMBER PROTECTION-COLLECTION AND USE BY PRIVATE BUSINESSES

COMMENTARY

This simple measure focuses on a going-forward basis on reducing the risk of identity theft from stolen SSNs by reducing the instances in which SSNs can be requested, collected, mailed, printed on wallet cards, used as passwords, and solicited over the Internet without encryption.

- **Stops most requests for, collection of, and mailing of the SSN.** Stops collection of the SSN by private businesses for purposes beyond credit, taxes, employment, investment, new bank accounts, child support and criminal record checks unless the SSN is required by law.
- **Stops these practices unless required by law:**
 - Placing SSNs on identification and membership cards
 - Posting, displaying, or making SSNs available to the general public
 - Using the SSN as a password or access code for goods and services.
 - Inviting input of the SSN on the web for unencrypted transmission.
- **Tailors exceptions for true need.** Some of the early state laws restricting SSN use included a variety of exceptions. Too many exceptions will undermine the usefulness of a state law restricting SSN collection and use.

SIMILAR LEGISLATION

Many states have enacted laws to restrict the printing on cards, mailing, display and Internet use of SSNs. For example, California enacted legislation in 2001 that generally prohibited businesses from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, mailing documents that display SSNs before the document is opened, printing SSNs

on cards necessary for accessing products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.¹ Twenty one states have passed laws similar to California’s—Arizona, Arkansas, Colorado, Connecticut, Georgia, Hawaii, Illinois, Maryland, Michigan, Minnesota, Missouri, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Texas, Utah, and Virginia.¹ Kansas and New Mexico have gone further and restricted the collection of SSNs.²

MODEL STATE SSN LAW ON PRIVATE COLLECTION, MAILING AND CERTAIN USES OF SSNS

Subsection A. Definitions. For purposes of this Act, the following terms have the following meanings:

- 1) “Social Security number” means any portion of three or more consecutive digits of a Social Security number.
- 2) “Person” means any individual, firm, partnership, association, corporation, limited liability company, organization or other entity, but does not include the state or any political subdivision of the state, or any agency thereof.

Subsection B. A person doing business in this State may not request, collect, or mail to the individual the Social Security number of an individual residing in this State unless one of the following exceptions applies.

- 1) The SSN is expressly required by federal, state, or local law or regulation.
- 2) The SSN is requested, collected or mailed in connection with a request for credit or a credit transaction initiated by the consumer or in connection with a lawful request for a consumer credit report.
- 3) The SSN is requested, collected or mailed in connection with the opening of a deposit account or in connection with an investment.

¹ See Arkansas (Ark. Code Ann. § 4-86-107 (2005)); Arizona (Ariz. Rev. Stat. § 44-1373 (2004)); Colorado (Colo. Rev. Stat. § 6-1-715(2006)); Connecticut (Conn. Gen. Stat. § 42-470 (2003)); Georgia (Ga. Code Ann. § 10-1-393.8 (2006)); Hawaii (Haw. Rev. Stat. § 487J-2 (2006)); (Illinois (815 Ill. Comp. Stat. 505/2QQ (2004)); Maryland (Md. Code Ann., Com. Law § 14-3301 et seq. (2005)); Michigan (Mich. Comp. Laws § 445.81 et seq. (2004)); Minnesota (Minn. Stat. § 325E.59 (2005)); Missouri (Mo. Rev. Stat. § 407.1355 (2003)); New Jersey (NJ Stat. Ann. § 56:8-164 (West 2005)); New Mexico (NM Stat. Ann. § 57-12B-4 (2005)); New York (N.Y. Gen. Bus. Law § 399-dd (2006)); North Carolina (N.C. Gen. Stat. § 75-62 (2005)); (Oklahoma (Okla. Stat. tit. 40, § 173.1 (2004)); Pennsylvania (74 Pa. Stat. Ann. § 201 (West 2006); Rhode Island (R.I. Gen. Laws § 6-48-8 (2006)); Texas (Tex. Bus. & Com. Code Ann. 35.58 (2003)); Utah (Utah Code Ann. § 31A-21-110 (2004)); and Virginia (Va. Code Ann. § 59.1-443.2 (2005)).

² Kansas recently passed legislation stating that businesses shall not “solicit, require or use for commercial purposes an individual’s social security number unless such number is necessary for such person’s normal course of business and there is a specific use for such number for which no other identifying number may be used.” Kan. Stat. Ann § 75-3520 (2006).

New Mexico also limits the collection of SSNs: “No business shall require a consumer’s social security number as a condition for the consumer to lease or purchase products, goods or services from the business.” (NM Stat. Ann. § 57-12B-3). This law permits businesses to require SSNs, however, “if the number will be used in a manner consistent with state or federal law or as part of an application for credit or in connection with annuity or insurance transactions” or “if the consumer consents to the acquisition or use.” (NM Stat. Ann. § 57-12B-3).

- 4) The SSN is requested, collected or mailed for purposes of employment, including in the course of the administration of a claim, benefit, or procedure related to the individual's employment by the person, including the individual's termination from employment, retirement from employment, injury suffered during the course of employment; or to check on an unemployment insurance claim of the individual.
- 5) The SSN is requested, collected or mailed for purposes of tax compliance.
- 6) The SSN is requested, collected, or mailed for the purpose of: interaction with a governmental law enforcement agency; the collection of child or spousal support; or to determine whether an individual has a criminal record.
- 7) Nothing in this section or section 2(d) prohibits a person from including his or her own Social Security number on materials sent through the mail. Nothing in this Act applies to the mailing of a copy of a public record which contains a Social Security number.

Subsection C. A person doing business in this State may not do any of the following with the Social Security number of an individual residing in this State unless expressly required to do so by federal, state, or local law or regulation:

- 1) Place the Social Security number of an individual on any card, tag, badge, or other device issued or used for identification or membership, or on other any card, tag or device issued to an individual, including one issued for the purpose of providing access to products or services. This section includes printing, embedding, encoding within a magnetic strip or on a chip, and any other means of placing the Social Security number on a card, tag, badge, or other device issued for identification or membership.
- 2) Solicit or require the use of the SSN as a password for computerized service, telephone customer service, or an Internet web site, or require that an individual provide his or her SSN as a condition to access goods, services, or a website.
- 3) Solicit or require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted, and the request or collection of the Social Security number is otherwise permitted under section (1).
- 4) Where mailing of a Social Security number is otherwise permitted under section 1), the Social Security number may not be printed on a postcard or other mailer that does not require an envelope, or in any other manner that makes the Social Security number visible on the envelope or without the envelope being opened.
- 5) Publicly post or display, or otherwise make available to the general public, including by sale to the general public, the Social Security number of another individual.

Subsection D. Penalties for violations of this Act.

- 1) A person who violates this section is responsible for the payment of a civil fine of not more than \$3,000 per violation.
- 2) A person who knowingly violates this section is guilty of a misdemeanor punishable by imprisonment for not more than 60 days or a fine of not more than \$3,000 or both.
- 3) A person who violates this section is liable to each person whose Social Security number is treated in violation of this Act for all of the following: \$5,000 per person, actual damages, and reasonable court costs and attorney’s fees to a prevailing plaintiff.

Subsection E. Severability. The provisions of this act are severable. If any phase, clause, sentence, provision or section is declared to be invalid or preempted in whole or in part by any federal law or regulation, the validity of the remainder of this Act shall not be affected.

SECTION 2: SECURITY FREEZE³

COMMENTARY

Identity thieves often use victims’ good credit history to open new accounts in victims’ names. Thieves fraudulently open a wide variety of accounts, including credit cards, loans, telephone service and other utilities, checking accounts, internet accounts, insurance, housing rental, other utilities and “other” accounts.⁴ These thieves then fail to pay the bills, causing the new creditors to pursue the victims and destroy the victims’ credit. This “new account fraud” costs businesses and consumers significantly more in time and money than “existing account fraud,” perhaps because it takes much longer to discover and to correct.⁵ Victims of new account fraud are also much more likely to suffer credit card problems, harassment by debt collectors, loan rejection, banking problems, insurance rejection, cut-off utilities, lawsuits, and criminal investigation.⁶

Generally, companies won’t open a new account unless they have reviewed the applicant’s consumer credit report or credit score derived from the

³ The security freeze is different from trade line blocking or fraud alerts under federal law. The federal Fair Credit Reporting Act provides that a consumer, subject to certain procedures, can act to “block” specific fraud-related items (or trade lines) from appearing in his or her consumer credit report. But trade line blocking does not prevent the issuance of a consumer credit report or credit score; it only limits certain fraud-related information from being included in the report. Similarly, a fraud alert attached to a report does not prevent issuing the report or a credit score. A fraud alert allows the potential creditor to get the report, but requires it merely to take conditions before the issuance of credit until certain identity verification procedures are complied with (or the issuer faces liability), but does not prevent the credit bureau from selling or sharing the report with potential new creditors. Conversely, a security freeze grants any consumer (whether or not a suspected or actual identity theft victim) the right to prevent the credit reporting agency from issuing his or her report or score for the purpose of issuing new credit or other new accounts. It freezes access to the report except for circumstances such as review of existing accounts and other limited purposes.

⁴ The Federal Trade Commission tracks identity theft reports and has identified all of these types of new account fraud. See http://www.consumer.gov/idtheft/pdf/synovate_report.pdf.

⁵ http://www.consumer.gov/idtheft/pdf/synovate_report.pdf

⁶ Id.

report. Once an identity thief supplies a victim’s personal information as part of an application for a new account, the potential creditor reviews the victim’s credit report or score and opens the new account. However, if the company where the identity thief tries to open a new account can’t get access to the victim’s credit report or score, the company will reject the fraudulent application for a new account. Only a state security freeze law allows consumers to lock up access to their credit files and to control who sees the file for the purpose of opening new accounts. In this way the security freeze empowers consumers to protect themselves from most types of new account fraud.

SIMILAR LEGISLATION:

Thirty-nine states and the District of Columbia have passed versions of security freeze legislation.⁷ Thirty-five of these states and the District of Columbia offer the security freeze to all consumers, which maximizes its value as a preventive tool for consumers while four states offer the freeze only to victims of identity theft.⁸ Many freeze laws now offer lower fees for placement and use of the freeze, and many state freeze laws permit electronic methods of freeze placement and lifting to enable rapid processing of requests to “thaw” or temporarily lift the freeze. The states still lacking any form of the security freeze as of August 2007 are Alabama, Arizona, Alaska, Idaho, Iowa, Michigan, Missouri, Ohio, Georgia, Virginia, and South Carolina.

MODEL STATE LAW

Subsection A. Definitions. For the purposes of this section, the following terms shall have the following meanings:

- 1) "Consumer reporting agency" means 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.
- 2) "Consumer credit report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit

⁷ Please see <http://www.consumersunion.org/pub/securityfreeze.htm>. Ark. Code Ann. §4-112-101 et seq.; Cal. Civ. Code § 1785.11.2; Colo.Rev.Stat. § 12-14.3-102, §§ 12-14-106.6 to 106.9; 2005 Conn. Pub. Acts 148; Del. Code Ann. tit. 6, §2203 (2007); D.C. Code § 28-3861; Fla. Stat. ch. 501.005; 2007 Haw. Sess. Laws 1612; 815 ILCS 505/2MM; Indiana Public Law No. 104 (2007); KS SB 196 (2006); Ky. Rev. Stat. Ann. 367.363 et. seq.; La. Rev. Stat. Ann § 9.3571(H) to (Y); 2005 Me. Laws 243; 2007 Md. Laws 52; 2007 Mass. Acts 4144; MN SB 2002 (2006); 2007 Miss. Laws 585; 2007 Mont. Laws 138; 2007 Neb. Laws 674; N.H. Rev. Stat. Ann. 359-B:24; NJ Pub. Law 2005, c. 226; N.M. Stat. Ann. § 56-15-3; NY CLS Gen Bus §380-a (k)-(n), §380-t; Nev. Rev. Stat. Ann. § 598C.300; 2005 N.C. Sess. Laws 243; N.D. Cent. Code, § 51-33-12; Okla. Stat. tit. 24, §149; 2007 Or. Laws 583; 73 Pa. Stat. Ann. § 2502; R.I. Gen. Laws §6-48-1; SD SB 180 (2006); 2007 Tenn. Pub. Acts 200; Tex. Bus. & Com. Code Ann. § 20.031 to 20.039 and 2007 Tex. Gen. Laws 222; Utah Code Ann. §13-45-102, 13-45-201 et seq.; 9 Vt. Stat. Ann. § 2480a to 2480j; 2005 Wash. Laws 342 and 2007 Wash. Laws 5826; W. Va. Code §46A-6L-101 et seq.; Wis. Stat. Ann. §100.54 (2005); Wyo. Stat. Ann. §40-12-501 et seq.

⁸ Arkansas, Kansas, Mississippi and South Dakota limit the option of using the security freeze to identity theft victims only.

worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

- a) credit or insurance to be used primarily for personal, family, or household purposes, except that nothing in this Act authorizes the use of credit evaluations, credit scoring or insurance scoring in the underwriting of personal lines of property or casualty insurance;
- b) employment purposes; or
- c) any other purpose authorized under section 15 U.S.C. § 1681b.

3) "Security freeze" means a notice, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer. If a security freeze is in place, such a report or information may not be released to a third party without prior express authorization from the consumer. This subdivision does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.⁹

4) "Reviewing the account" or "account review" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Subsection B. Security Freeze: Timing, Covered Entities, Cost.

- 1) A consumer may elect to place a "security freeze" on his or her consumer credit report by any of the following, at the option of the consumer:
 - a) making a request by mail,¹⁰
 - b) making a request by telephone by providing certain personal identification, or
 - c) making a request directly to the consumer reporting agency through a secure website or secure electronic mail connection.. Consumer reporting agencies shall make a secure website or secure electronic mail method of requesting a security freeze available by this Act's effective date.¹¹

⁹ This definition ensures that the freeze stops access, except on permission by the consumer, to both the consumer's credit report and information derived from it, such as the credit score. The credit score must be included because some types of new accounts can be opened based on a credit score without examination of the consumer credit report.

¹⁰ Certified mail adds expense and time for consumers to place the freeze, but does not provide proof of identity. The model act now permits the use of regular mail. A consumer who wants the mail to be tracked may still make a personal choice to use a different method. Delaware, Montana, New Mexico all currently allow placement by regular mail; Indiana, Massachusetts and Oregon will do so on their enactment dates. The District of Columbia requires a method of placement either by mail or by telephone instead of certified mail by 1/31/09. Wyoming requires both an electronic contact method and telephone placement by 9/1/08, and Maryland requires placement by telephone, email or secure electronic connection by 1/1/10. Utah requires an electronic contact method for placement by 9/01/08. Montana, Tennessee and West Virginia require placement by secure electronic method by 1/31/09. New Mexico and North Dakota require placement by telephone or secure electronic method if they are made available by the credit reporting agencies.

¹¹ Right now, the credit reporting agencies have secure websites set up that enable a consumer to identify themselves to the satisfaction of the credit reporting agency, which then is willing to provide the consumer a copy of his or her consumer credit report. Consumers should have the option at that stage to allow a consumer to freeze and unfreeze their report.

- 2) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than three business days after receiving a request by mail. Requests by telephone, secure website or secure electronic mail shall be honored within 15 minutes after the request has been completed beginning September 1, 2008. Within one year of this Act's effective date, a consumer reporting agency shall place a security freeze on a consumer's credit report no later than 24 hours after receiving the request for placing the freeze by mail.¹²
- 3) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within three business days of placing the freeze and at the same time shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her consumer credit report or credit score for a specific party or period of time, or when permanently lifting the freeze. Within one year of this Act's effective date, the consumer reporting agency shall send such a written confirmation and unique personal identification number or password to the consumer no later than 24 hours after receiving the request after placing the freeze.
- 4) If the consumer wishes to allow his or her consumer credit report or credit score to be accessed for a specific party or period of time while a freeze is in place, he or she shall contact the consumer reporting agency via telephone, mail, secure website or secure electronic mail,¹³ with a request that the freeze be temporarily lifted, and provide the following:
 - a) proper identification,
 - b) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (3) of subsection B, and
 - c) the proper information regarding the third party who is to receive the consumer credit report or credit score for the time period for which the report shall be available to users of the consumer credit report or credit score.¹⁴
- 5) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a consumer credit report and credit score pursuant to paragraph (4) of subsection (B) shall comply with the request no later than three business days after receiving the request by mail or no later than 15 minutes if after receiving the request by electronic mail or by telephone beginning September 1, 2008.¹⁵ Within one year of this Act's effective date,

¹² Montana Legislation SB 116 and North Dakota HB 1417.

¹³ See footnote 12, above and footnote 17, below.

¹⁴ A consumer must lift, or "thaw," a freeze to open a new account, however, when access to the report is thawed, the consumer is vulnerable to new account fraud. Thawing the report for a specific time frame gives the consumer versatility to open multiple new accounts, but puts him at greatest risk; thawing for a specific potential creditor creates minimal risk because it facilitates opening only that particular account. Twenty-one states and the District of Columbia give consumers both options for managing their freeze. Arkansas, Delaware, Florida, Kansas, Kentucky, Louisiana, Nebraska, North Carolina, Oklahoma, Oregon, Rhode Island, South Dakota, Tennessee, Utah, Washington, West Virginia, Wisconsin and Wyoming allow the freeze to be thawed for specific time periods only.

¹⁵ This model requires near instant thawing of a security freeze at the consumer's request. That goal will make the freeze more convenient to both consumers and retailers who are selling goods on credit. The District of Columbia,

a consumer reporting agency shall honor such a request no later than 24 hours after receiving the request by mail.

- 6) A consumer reporting agency shall develop procedures involving the use of telephone, fax, or, by a secure electronic connection or method to receive and process a request from a consumer to temporarily lift a freeze on a consumer credit report or credit score pursuant to paragraph (4) of subsection (B) in an expedited manner.
- 7) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:
upon consumer request; or if the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a consumer's credit report, the consumer reporting agency shall notify the consumer in writing five business days prior to removing the freeze on the consumer's credit report.
- 8) If a third party requests access to a consumer credit report or credit score on which a security freeze is in effect, and the consumer does not allow his or her consumer credit report or credit score to be accessed for that specific party or period of time, the third party may treat the application as incomplete.
- 9) A security freeze shall remain in place without assessment of any fees unless a fee for a lost personal identification number or password is permitted under paragraph (13) is charged, until the consumer requests that the security freeze be removed. A consumer reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides both of the following:
 - a) proper identification, and
 - b) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (3) of subsection (B).
Not later than one year after the effective date of this Act, a consumer reporting agency shall remove a security freeze 24 hours after receiving such a request.
- 10) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.
- 11) A consumer reporting agency may not suggest or otherwise state or imply to a third party that the consumer's security freeze reflects a negative credit score, history, report or rating.
- 12) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

Delaware, Indiana, Maryland, Montana, Nebraska, Tennessee, Utah, Washington and Wyoming have passed laws that require a 15 minute lift. A 15 minute lift must be provided to Tennessee, Utah, DC, Washington and Wyoming residents beginning 9/1/2008. The laws in Delaware, Maryland, Montana and Nebraska are effective January 31, 2009. At least one credit reporting agency has been quoted as saying they already thaw freeze requests within 15 minutes, emphasizing the feasibility of this feature. *See*, "R.I. Gives Consumers Right to Freeze Credit Report," by Natalie Myers, Providence Business News, July 8, 2006, issue 21-13.

- a) a person, or the person's subsidiary, affiliate, agent, or assignee with which the consumer has or, prior to assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt.
 - b) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under paragraph (4) of subsection (B) for purposes of facilitating the extension of credit or other permissible use.
 - c) any person acting pursuant to a court order, warrant, or subpoena.
 - d) a State or local agency which administers a program for establishing and enforcing child support obligations.
 - e) the [state health department] or its agents or assigns acting to investigate fraud.
 - f) the [state tax authority] or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities.
 - g) a consumer reporting agency for its database or file that consists entirely of the following, and is used solely for, one or more of the following: criminal record information, tenant screening, employment screening, or fraud prevention and detection.
 - h) a person for the purposes of prescreening as defined by the federal Fair Credit Reporting Act.
 - i) any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed.
 - j) any person or entity for the purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.
- 13) A consumer may not be charged for any security freeze services, including but not limited to the placement, temporarily lifting or removing of a security freeze. A consumer, however, can be charged no more than \$5 only in the following discrete circumstance:
- a) If the consumer fails to retain the original personal identification number provided by the agency, the consumer may not be charged for a one-time reissue of the same or a new personal identification number; however, the consumer may be charged no more than \$5 for subsequent instances of loss of the personal identification number.¹⁶

¹⁶ Fees are a major barrier to security freeze use and are thus contrary to the fraud prevention policy embodied by the security freeze. For a consumer to place the freeze on his or her credit files, he or she must do it at all three national credit reporting agencies, and possibly regional ones as well. Thus a \$5 fee really functions like a \$15 fee, and a \$15 fee results in a \$45 charge. These amounts are very significant, particularly if they are tied to thawing the freeze temporarily. California, Delaware, District of Columbia, Florida, Hawaii, Indiana, Illinois, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming make all aspects of security freezes free to victims. Massachusetts also offers the freeze for free for spouses of identity theft victims. Louisiana also makes them free for their citizens 62 years of age or older. Florida, Illinois, New Mexico, Oklahoma, Pennsylvania and Rhode Island make the freeze free for their citizens aged 65 or older. The best state laws on security freeze fees overall are Indiana, which makes it free of charge to place, temporarily lift, or removal a freeze; Montana, which charges \$3 for placing or temporarily lifting the freeze and free to remove the freeze; New Jersey, which makes placing a freeze free and caps the fee to thaw a freeze or replace a password at \$5. For another approach, Tennessee residents pay a \$7.50 fee to place the freeze, no fees to temporarily lift the freeze and \$5 to permanently remove the freeze.

Subsection C. Notice of Rights. At any time that a consumer is required to receive a summary of rights required under Section 609 of the federal Fair Credit Reporting Act or under [state law], the following notice shall be included:

[State] Consumers Have the Right to Obtain a Security Freeze

You may obtain a security freeze on your consumer credit report at no charge to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a “security freeze” on your consumer credit report pursuant to [State law].

The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your consumer credit report, within five business days (and by [date], no later than one business day) you will be provided a personal identification number or password to use if you choose to remove the freeze on your consumer credit report or to temporarily authorize the release of your consumer credit report or credit score for a specific party, parties or period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the third party or parties who are to receive the consumer credit report and credit score or the period of time for which the report shall be available to users of the consumer credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a consumer credit report shall comply with the request no later than three business days after receiving the request by mail and no later than 15 minutes after receiving the request by telephone or by electronic mail beginning September 1, 2008. (By [date] the consumer reporting agency must temporarily lift the freeze within 1 business day of receiving the request by mail.)

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze – either completely if you are shopping around, or specifically for a certain creditor – with enough advance notice before you apply for new credit for the lifting to take effect. Until [date], you should lift

the freeze at least 3 business days before applying; between [date] and [date] you should lift the freeze at least one business day before applying; and after [date] you should lift the freeze at least 15 minutes before applying for a new account.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.”¹⁷

Subsection D. Violations; Penalties.

If a consumer reporting agency, violates the security freeze by releasing a consumer credit report or information derived from a consumer credit report that has been placed under a security freeze, the affected consumer is entitled to:

- 1) Notification within five business days of the release of the information, including specificity as to the information released and the third party recipient of the information.
- 2) File a complaint with the Federal Trade Commission and the state Attorney General and [other state consumer protection agency].
- 3) In a civil action against the consumer reporting agency to recover:
 - a) injunctive relief to prevent or restrain further violation of the security freeze, and/or
 - b) a civil penalty in an amount not to exceed \$5,000 for each violation plus any damages available under other civil laws, and
 - c) reasonable expenses, court costs, investigative costs, and attorney’s fees, and
 - d) punitive damages
- 4) Each violation of the security freeze shall be counted as a separate incident for purposes of imposing penalties under this section.

Subsection E. Severability.

The provisions of this Act are severable. If any phrase, clause, sentence, provision or section is declared to be invalid or preempted, in whole or in part, by federal law or regulation, the validity of the remainder of this Act shall not be affected thereby.

SECTION 4: PREVENTION OF AND PROTECTION FROM SECURITY BREACHES

COMMENTARY

According to the Privacy Rights Clearinghouse, more than 645 data security breaches have been reported from January 2005 through August 2007,

¹⁷ Consumers need to know about the freeze in order to decide whether to use it. This notice is given when other laws require consumer reporting agencies to give notice of other rights. Arkansas, California, Colorado, Delaware, District of Columbia, Florida, Hawaii, Illinois, Indiana, Maryland, Massachusetts, Montana, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oklahoma, Rhode Island, Tennessee, Vermont, West Virginia and Wisconsin require this notice be provided.

involving over 159 million customer records.¹⁸ These security breaches included financial institutions, data brokers, businesses, government agencies and universities. The model notice of breach law is based on the premise that a company or government agency that has had a security breach should not get to decide whether or not to notify consumers about the breach.

Business and government should protect data and work toward establishing security procedures to maintain the confidentiality and integrity of that data to prevent security breaches. When a data breach does occur, the law should require notice to all consumers in the event that personal data has, or may have been, compromised. For consumers, notice of all breaches is necessary so that they can take measures to protect themselves from identity theft, such as placing a fraud alert or security freeze on their consumer credit report and taking extra care when reviewing account statements.

SIMILAR LEGISLATION

Most states have passed notice of data security breach legislation. The following states have passed the best laws, enacting legislation similar to the model language requiring consumers to be notified when a breach of data has occurred: California, Illinois, Minnesota, Nevada, New York, North Dakota, and Texas.¹⁹

MODEL STATE LAW

Subsection A. Definitions. For the purposes of this section, the following terms shall have the following meanings:

- 1) “Person” means any individual, firm, partnership, association, corporation, limited liability company, organization or other entity, but does not include the state or any political subdivision of the state, or any agency thereof.
- 2) “Entity” a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.
- 3) “Breach of the security of the data” means unauthorized acquisition of computerized or non-computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. Good faith acquisition of personal information by an employee or agent of the entity for a legitimate purpose of the entity is not a breach of the security

¹⁸ “A Chronology of Data Breaches Reported Since the ChoicePoint Incident”

www.privacyrights.org/ar/ChronDataBreaches.htm This number reflects the number of records that have been compromised as a result of a data breach and not necessarily the number of individuals that have been affected. Some individuals might have been victims of more than one data security breach.

¹⁹ Cal. Civil Code § 1798.80 – 1798.82; 815 ILCS 530/1; Minn. Stat. 325E.61 et seq.; N.Y. Gen. Bus. Law §899-aa; NRS 603A.010 et seq; ND Cent. Code 51-30-01 to 07; and Tex. Bus & Com. Code Ann. 4-48-103 .

of the data, provided that the personal information is not used for a purpose unrelated to the entity or subject to further unauthorized disclosure. Breach of the security of non-computerized data includes but is not limited to unauthorized photocopying, facsimiles, or other paper-based transmittal of documents.

- 4) “Personal information” means an individual’s last name, address, or phone number in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted, or encrypted with an encryption key that was also acquired:
 - a) Social Security number.
 - b) Driver’s license number or state identification card number.
 - c) Account number, credit, debit, or other number identifying a payment device, if circumstances exist in which such a number could be used without additional identifying information, access codes, or passwords.
 - d) Account passwords or personal identification numbers (PINs) or other access codes.
 - e) Biometric data, other than a photograph.
 - f) Any of item (a)-(e) when not in connection with the individual’s last name, address or phone number if the information compromised would be sufficient to perform or attempt to perform identity theft or other illegal conduct against the person whose information was compromised. “Personal information” does not include information that is lawfully obtained from a single public record of federal, state, or local government record, provided that such information has not been aggregated or consolidated into an electronic database or similar system by the entity.²⁰
- 5) “Credit card” has the same meaning as in section 103 of the Truth in Lending Act.²¹
- 6) “Debit card” means any card or device issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account holding assets of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services.
- 7) “Payment device” means a card, code, or other means to access or place a charge on a consumer’s account or bill.
- 8) “Social Security number” means any portion of three or more consecutive digits of a Social Security number.

Subsection B. Notice of Breach.

²⁰ The model law’s definition of personal information has been expanded as a result of improvements made by North Carolina’s law which includes any form of data, including biometric data and New York’s inclusion of information which has been encrypted if the encryption key that has also been acquired.

²¹ 15 U.S.C. § 1601 *et. seq.*

- 1) Except as provided in paragraph 2 of subsection B, any person or entity²² that owns or uses personal information in any form (whether computerized, paper, or otherwise) that includes personal information concerning a [State] resident shall notify the resident that there has been a breach of the security of the data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (2) of subsection B, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

- 2) The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may materially impede a criminal investigation.

- 3) For purposes of this section, “notice” to consumers may be provided by one of the following methods:
 - a) Written notice.
 - b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, for notices legally required to be in writing, set forth in Section 7001 of Title 15 of the United States Code.
 - c) Substitute notice, if the agency demonstrates that the cost of providing notice to persons in this state would exceed _____ (\$_____) or that the affected class of subject persons to be notified in this state exceeds _____²³ or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
 1. Conspicuous posting of the notice on the Internet site of the agency or person, if the agency or person maintains a public Internet site; and

 2. Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual’s personal data is included in the security breach.

- 4) Content of Notice

Such notice shall include--

 - a) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person, including social security numbers, driver’s license or State identification numbers and financial data;

 - b) a toll-free number--

²² Any person or entity may include but is not limited to government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity which, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personal information.

²³ The threshold numbers for substitute notice may depend on the state’s population and size. For instance, California, Illinois allow substitute notice when the cost exceeds \$250,000 or the affected class of persons to notify in their respective states exceeds 500,000. Smaller states like New Hampshire and Vermont allow substitute notice when the cost exceeds \$5,000 or the affected class of persons to notify in their respective states exceeds 1,000.

1. that the individual may use to contact the agency or person, or the agent of the agency or person; and
2. from which the individual may learn--
 - (a) what types of information the agency or person maintained about that individual or about individuals in general; and
 - (b) whether or not the agency or person maintained information about that individual; and
 - (c) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.
- 5) The notification required by this section may be delayed if a law enforcement agency determines, in writing, that the notification may seriously impede a criminal investigation. This notification shall state the duration of the delay requested, or must be renewed after 90 days.
- 6) **Additional Obligation Following Breach --** A person required to provide notification under Subsection A shall provide or arrange for the provision of, to each individual to whom notification is provided under Subsection B and on request and at no cost to such individual to either provide at the choice of the consumer credit reports from at least one of the major credit reporting agencies beginning not later than 2 months following a breach of security and continuing on a quarterly basis for a period of 2 years thereafter or pay for freeze fees, which include placement with each of the major nationwide credit reporting agencies and temporary lift twice per credit reporting agency during a 12 month period.

Subsection C. Enforcement.

The attorney general may enforce this chapter. The attorney general, in enforcing this section.

Subsection D. Waiver. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

SECTION 5: RIGHT TO FILE A POLICE REPORT REGARDING IDENTITY THEFT

COMMENTARY

When a consumer suspects that he or she has been the victim of identity theft, his or her most obvious recourse is the local police department. Whether the theft has occurred at home or in another community, a consumer should be entitled to file a police report in his or her home jurisdiction. The local police department or law enforcement agency may choose to forward the report or information therein to the proper authorities in another jurisdiction.

Consumers need police reports to get access to their federal right to get

records of transactions from a business where the thief did business while impersonating the consumer.²⁴

SIMILAR LEGISLATION

Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Illinois, Iowa, Louisiana, Maryland, Michigan, Minnesota, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Pennsylvania, South Dakota, Vermont, the Virgin Islands and Washington all have state laws requiring that local police departments take police reports.²⁵ Many other states refer to the admissibility of police reports in identity theft prosecutions, but do not have laws requiring police departments to take such reports.²⁶

MODEL STATE LAW

A. A person who has learned or reasonably suspects that he or she has been the victim of identity theft may contact the local law enforcement agency that has jurisdiction over his or her actual residence, which shall take a police report of the matter, and provide the complainant with a copy of that report. Notwithstanding the fact that jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, the local law enforcement agency shall take the complaint and provide the complainant with a copy of the complaint and may refer the complaint to a law enforcement agency in that different jurisdiction.

B. Nothing in this section interferes with the discretion of a local police department to allocate resources for investigations of crimes. A complaint filed under this section is not required to be counted as an open case for purposes such as compiling open case statistics.

SECTION 6: ADEQUATE DESTRUCTION OF PERSONAL RECORDS

COMMENTARY

In order to prevent sensitive personal information from falling into the hands of identity thieves, states should require businesses to properly dispose of records containing information that could be used to impersonate an individual. The Fair Credit Reporting Act (FCRA) and its implementing

²⁴ 15 U.S.C. §1681g.

²⁵ Ark. Code Ann. §5-37-228; Cal. Penal Code § 530.6; Co. Rev. Stat. §16-5-103; Conn. Gen. Stat. §54-1n; 6 Del. Laws 2204; D.C. Code Ann. § 22-3227.08; 720 Ill. Comp. Stat. § 5/16G-30; Iowa Code §715.8; La. Stat. Ann. § 9:3568; Md. Code. Ann. Crim § 8-304; Mich. Stat. Ann. § 780.754a; Minn. Stat. §609.527(2002); N.H. Rev. Stat. Ann. §359-B:29; N.J. Stat. Ann. §2C:21-17.6; 2007 NY Laws 346; N.C. Gen. Stat. §14-113.21A; N.D. Cent. Code §51-31-04; 18 Pa.C.S. § 4120e; S.D. Codified Laws §22-40-10; Vt. Stat. Ann. tit. 9 § 2480k; V.I. Code Ann. §14-42:110-2206; Wash. Rev. Code §9.35.020. *See also*, Letter from Consumer Groups, *Re: Request to State Attorneys General to Act to Assist Identity Theft Victims in Using New Federal Rights*, January 15, 2004. Available at: <http://www.epic.org/privacy/fcra/factagltr1.15.04.pdf>.

²⁶ In addition to allowing victims to file reports with their local police departments, states may also want to consider modifying their identity theft criminal statutes to define identity theft as occurring where the victim resides, where the perpetrator resides, where the incidents occurred, and/or at any other place instrumental to the completion of the offense.

regulations require proper disposal only of that consumer information which is derived from consumer credit reports. There is no federal law generally requiring proper disposal of all business records containing sensitive personal information of individuals. This model state law requires businesses to take reasonable measures to protect against unauthorized access to or use of records containing personal information when disposing of them. In addition, it extends this requirement to any third-party vendors engaged to dispose of such records. The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., does not preempt states from enacting such provisions; in fact, it explicitly states that the federal disposal provision shall not be construed to alter or affect any disposal requirement imposed under any other law.

SIMILAR LEGISLATION

Several states, including Arkansas, California, Georgia, Hawaii, Kentucky, Montana, Nevada, New Jersey, New York, North Carolina, Oregon, Texas, Utah, Washington and Wisconsin have enacted legislation similar to this model.²⁷

MODEL STATE LAW²⁸

Subsection A. Definitions. For the purposes of this section, the following terms shall have the following meanings:

- 1) “Business” means sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity that destroys records.
- 2) “Dispose” includes:
 - (a) the discarding or abandonment of records containing personal information, and
 - (b) the sale, donation, discarding or transfer of any medium, including computer equipment, or computer media, containing records of personal information, or other non-paper media upon which records of personal information is stored, or other equipment for non-paper storage of information.
- 3) “Personal Information” means a social security number; a personal

²⁷ Ark. Code Ann. §4-110-104 (2005); Cal. Civil Code Ann. § 1798.80 – 1798.84; Ga. Code Ann. § 10-15-1, 10-15-2; Haw. Rev. Stat. §487R-2; KY. Rev. Stat. Ann. §365.725; Mont. Code. Ann. § 30-14-703; Nev. Rev. Stat. 603A.200; N.C. Gen Stat. §75-64 et seq.; N.J. Stat. § 56:8-162; NY CLS Gen Bus § 399-h; 2007 Ore. SB 583; 2007 Mass. Laws 4144; Tex. Code. Ann. §48.102; Utah Code Ann. §13-44-201 (2006); Wash. Rev. Code §19.215.020; Wis. Stat. § 895.505 (statute applies to financial institutions, medical businesses, and tax preparation businesses). Colorado requires both public and private entities to develop policies for the destruction or proper disposal of documents containing personal information. C.R.S. § 6-1-713.

²⁸ Modeled on FCRA, which complies by treating these records the same as credit report information.

identification number; a password; a passcode; an official state or government-issued driver's license or identification card number; a government passport number; biometric information other than a photographic image; an employer, student, or military identification number; a financial transaction device or financial account number, or health information including medical records and health insurance identifiers.

- 4) "Records" means any material on which written, drawn, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.
- 5) "Social Security number" means any portion of three or more consecutive digits of a Social Security number.

Subsection B. Disposal of Records Containing Personal Information. Any business that conducts business in [state] and any business that maintains or otherwise possesses personal information of residents of [state] must take all reasonable measures to protect against unauthorized access to or use of the information in connection with, or after its disposal. Such reasonable measures must include, but may not be limited to:

- 1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed;
- 2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other non-paper media containing personal information so that the information cannot practicably be read or reconstructed;
- 3) After due diligence, entering into and monitoring compliance with a written contract with another party engaged in the business of record destruction to dispose of personal information in a manner consistent with this statute. Due diligence should ordinarily include, but may not be limited to, one or more of the following: reviewing an independent audit of the disposal company's operations and/or its compliance with this statute or its equivalent; obtaining information about the disposal company from several references or other reliable sources and requiring that the disposal company be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal company;
- 4) For disposal companies explicitly hired to dispose of records containing personal information: implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of

personal information during or after the collection and transportation and disposing of such information in accordance with examples (1) and (2) above.

Subsection C. Business Policy. Procedures relating to the adequate destruction or proper disposal of personal records must be comprehensively described and classified as official policy in the writings of the business entity, including corporate and employee handbooks and similar corporate documents.

Subsection D. Penalties and Civil Liability

- 1) Any person or business that violates this section may be subject to a civil penalty of not more than \$3,000.
- 2) Any individual aggrieved by a violation of this section may bring a civil action in [State court] to enjoin further violations and to recover actual damages, costs, and reasonable attorney's fees.

SECTION 7: SEVERABILITY CLAUSE

COMMENTARY

States should include this clause in any portion of this model bill that they choose to enact.

MODEL STATE LAW

The provisions of this Act are severable. If any phrase, clause, sentence, provision or section is declared to be invalid or preempted, in whole or in part, by federal law or regulation, the validity of the remainder of this Act shall not be affected thereby.

|

For additional background information:

After the FACT ACT: What States Can Still Do to Prevent Identity Theft
Gail Hillebrand, Senior Attorney, Consumers Union

Which is available at:

<http://www.consumersunion.org/creditmatters/creditmattersupdates/001640.html>

¹ Cal. Civil Code § 1798.85 (West 2001).