

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

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

**Editors:**

**Ed Mierzwinski, Abigail Caplovitz, Kerry Smith and Sarah Ackerstein of the  
state PIRGs**

**Gail Hillebrand and Michelle Jun of Consumers Union**

**Updated November 2005<sup>1</sup>**

---

<sup>1</sup> Sections 2(B)(1)(a) and 2(B)(4) of this Model Act were updated 23 January 2006.

**SUMMARY**

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act).<sup>2</sup> With the FACT Act, Congress significantly amended the Fair Credit Reporting Act (FCRA)<sup>3</sup>, which provides consumer protections regarding the use, accuracy, and privacy of consumer credit reports. Through its passage, the financial industry won its primary goal: permanent preemption of stronger state credit and privacy laws in several, but importantly, not all, areas.

Congress did not complete the job of protecting citizens from identity theft or credit bureau mistakes when it enacted the FACT Act. Instead, the federal FACT Act allows states to take additional steps to reduce identity theft.

The State Clean Credit and Identity Theft Protection Act offers specific, workable provisions that state legislatures can adopt to reduce the risk of identity theft and to give consumers tools to prevent some of the harm from identity theft. The model law offers types of protections and of these that have actually been adopted by state legislatures.

The model law proposes additional safeguards in some of the numerous areas which the 2003 federal FACT Act left for future action by the states. The model law's provisions address some of areas where federal law permits states to give consumers greater protection. The Appendix provides an extensive analysis of the authority of states to enact laws in the areas covered by this model law.

We welcome information about enhancements and other approaches being considered in the states. The authors are available to discuss the model law and its features with state legislators and staff, and to provide other appropriate assistance. Please contact Ed Mierzwinski ([edm@pirg.org](mailto:edm@pirg.org)) or (202) 546-9707x314 or NJPIRG staffer Abigail Caplovitz at (609) 394-8155, or Gail Hillebrand or Michelle Jun at Consumers Union, (415) 431-6747. We are indebted to Kerry Smith, a former PIRG staffer, and to Sarah Ackerstein, a former intern at the national office of the state PIRGs, U.S.PIRG for their significant contributions to the model act.

-Ed Mierzwinski and Gail Hillebrand

---

<sup>2</sup> Fair and Accurate Credit Transactions Act (FCRA), Pub. L. No. 108-159, 2003 HR 2622 (2003).

<sup>3</sup> Fair Credit Reporting Act, 15 U.S.C.A. § 1681 *et. seq.*

**INTRODUCTION**

What this model law does:

This model identity theft legislation has been compiled with the intent to put forth the best language and practices in providing 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 2005 revision are updates to reflect improvements that have been adopted, or considered, in state legislatures. The model act addresses the following in eleven sections:

- Definitions;
- Security Freeze;
- Protection for Credit Header Information;
- Right to File a Police Report Regarding Identity Theft;
- Factual Declaration of Innocence After Identity Theft;
- Consumer-Driven Credit Monitoring;
- Prevention of and Protection From Security Breaches;
- Social Security Number Protection;
- Banning Credit Scoring and Insurance Scoring for Use in Insurance Decisions;
- Adequate Destruction of Personal Records; and
- Severability Clause.

Background:

Credit bureaus collect and compile information about consumer creditworthiness from banks and other creditors and from public record sources such as lawsuits, bankruptcy filings, tax liens and legal judgments. The three major credit bureaus—Experian, Equifax, and Trans Union— maintain files on nearly 90 percent of all American adults. Those files are routinely sold to credit grantors, landlords, employers, insurance companies, and many others interested in the credit record of a consumer, often without the consumer's knowledge or permission. Several studies since the early 1990s have documented sloppy credit bureau practices that lead to mistakes on credit reports—for which consumers pay the price. The most recent study of credit reports by the state PIRGs found that twenty-five percent of surveyed reports contained serious errors that could result in the denial of credit, such as false delinquencies or accounts that did not belong to the consumer.<sup>4</sup> Other reports have found similar problems with credit reports.<sup>5</sup>

<sup>4</sup> State PIRGs, *Mistakes Do Happen*, June 2004, available at: <http://uspirg.org/reports/MistakesDoHappen2004.pdf>

<sup>5</sup> See, Consumers Union, *What Are They Saying About Me? The Results of a Review of 161 Credit Reports from the Three Major Credit Bureaus*, April 29, 1991; Consumer Federation of America and National Credit Reporting Association, *Credit Score Accuracy and Implications for Consumers*, December 2002, available at: [http://www.consumerfed.org/121702CFA\\_NCRA\\_Credit\\_Score\\_Report\\_Final.pdf](http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf); and Robert Avery, Paul Calem, Glenn Canner, and Raphael Bostic, “An Overview of Consumer Data and Credit Reporting,” *Federal Reserve Bulletin*, February 2003, available at: <http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf>. We have reviewed the follow-up study by Avery, Calem and Canner, “Credit Report Accuracy and Access to Credit,” *Federal Reserve*

Consumers with serious errors in their credit reports can be denied credit, home loans, apartment rentals, auto insurance, or even medical coverage and the right to open a bank account or use a debit card. Consumers with serious errors in their reports who do obtain credit or a loan may have to pay higher interest rates because the mistakes falsely place them in the sub-prime, high-cost lending pool.

Some of the errors in credit reports are the result of identity theft. Identity theft is the taking of another's personal information –such as social security number, name or date of birth—for the purpose of assuming the victim's identity to commit fraud. It has been called one of the fastest growing crimes. In September 2003, the Federal Trade Commission released a survey showing that 27.3 million Americans have been victims of identity theft in the previous five years, including 9.9 million people in the previous year alone.<sup>6</sup> According to the survey, identity theft costs businesses and financial institutions nearly \$48 billion and consumer victims reported \$5 billion in out-of-pocket expenses in 2002 alone.

Longstanding role of the states in credit report issues:

States have long taken the lead in protecting consumers' privacy and ensuring the accuracy of credit reports. In 1992, Vermont was the first state to pass a law providing a free annual credit report on request, followed by Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey. California adopted other comprehensive reforms in 1994. California later became the first state to require disclosure of credit scores and protections for identity theft victims. In 2003, Congress followed the states' lead in these areas, adopting the free credit report and access to a credit score as well as enacting some new identity theft protections.

Federal context:

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act).<sup>7</sup> With the FACT Act, Congress significantly amended the Fair Credit Reporting Act (FCRA)<sup>8</sup>, which provides consumer protections regarding the use, accuracy, and privacy of consumer credit reports. Through its passage, the financial industry won its primary goal: permanent preemption of stronger state credit and privacy laws in several, but importantly, not all areas. The FACT Act also included several modest consumer reforms, including the right to a free annual credit report on request from national credit bureaus and new requirements to increase the accuracy of reports. However, these improvements come at the very high and unacceptable price of preemption of some types of

---

*Bulletin*, Summer 2004, pages 297-322. We disagree with the inferences some have made that this study concludes that the credit bureaus could not do a much better job. In fact, the Federal Reserve study points out that nearly 33% of consumers have missing information in at least one account. The study also makes clear, among other concerns, that some individuals are more affected by errors than others; specifically, individuals with lower scores are more likely to be hurt by mistakes and that false or duplicative collection accounts have a significant negative impact. *See*,

[http://www.federalreserve.gov/pubs/bulletin/2004/summer04\\_credit.pdf](http://www.federalreserve.gov/pubs/bulletin/2004/summer04_credit.pdf)

<sup>6</sup> Federal Trade Commission, *Identity Theft Survey Report*, Sept. 2003, available at:

<http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

<sup>7</sup> Fair and Accurate Credit Transactions Act (FACTA), Pub. L. No. 108-159, 2003 HR 2622 (2003).

<sup>8</sup> Fair Credit Reporting Act, 15 U.S.C.A. § 1681 *et. seq.*

state laws. In addition, many of the new consumer protections provided in the 2003 amendments solely rely on agency enforcement and explicitly do not allow consumers a federal right of action to sue violators.

Fortunately, the federal FACT Act did not interfere with most state authority to prevent and mitigate identity theft, to protect from unfair use of credit scoring, to require that personal data be held securely, and to require that consumers be notified when there has been a breach in the security of their personal information. While some areas of state authority are preempted under the revised FCRA, many are not. This model law offers language in areas that states remain free to address.

This model law is intended for use with the companion document, *After the FACT Act: What the States Still Can Do to Prevent Identity Theft*, a legal memorandum by Gail Hillebrand of Consumers Union.<sup>9</sup> The memorandum discusses and analyzes the various forms of preemption under the federal Fair Credit Reporting Act and describes the powers the Act reserves to the states.

Practical considerations:

Each section of this model law has an introduction, explains the section and describes similar state laws. Some of the sections also contain explanatory footnotes. The footnotes are not part of the model legislation text.

The proposals below are not intended to be all-inclusive; states should contact us with other ideas they believe fall outside the FCRA's preemption provisions. However, the model act offers a starting point to enhance consumer protection against identity theft and intrusions into personal data.

The model law is organized into nine related laws, which can be enacted as discrete, separate pieces of legislation or as a single package. The discussion of each section describes existing state laws that reflect the concepts offered in the model law, with citations to those state laws. If enacting a provision separately, states should use any definitions from section one that are referenced in that provision. For example, if filing stand-alone legislation restricting the use of credit header information, include the definition of "credit header" from section one as well as the substantive language of section three. In addition, states should include the severability clause outlined in section eleven of the model law when enacting any of its provisions.

---

<sup>9</sup> This memorandum is included as an Appendix to this document. It also is available at: <http://www.consumersunion.org/creditmatters/creditmattersupdates/001640.html>.

**SECTION 1: DEFINITIONS<sup>10</sup>**

For the purposes of this article, the following terms shall have the following meanings:

- A. The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.
- B. "Consumer" means an individual.
- C. "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.
- D. "Consumer report" or "credit report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit 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:
  - 1) 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;
  - 2) employment purposes; or
  - 3) any other purpose authorized under section 15 U.S.C. § 1681b.
- E. "Credit card" has the same meaning as in section 103 of the Truth in Lending Act.<sup>11</sup>
- F. "Credit header information" means written, oral, or other communication of any information by a consumer reporting agency regarding the social security number of the consumer, or any derivative thereof, and any other personally identifiable information of the consumer that is derived using any nonpublic personal information, except the name, address, and telephone number of the consumer if all are listed in a residential telephone directory available in the locality of the consumer.

---

<sup>10</sup> Many of these definitions were taken from federal law, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Truth-in-Lending Act. A state legislative counsel's office should modify these federal definitions, citations and references to local needs as appropriate. Additional definitions are offered in other sections. If enacting a provision separately, states should use any definitions from section one that are referenced in that provision. For example, if filing stand-alone legislation restricting the use of credit header information, states will need to include the definition of "credit header" from section one as well as the substantive language of section three.

<sup>11</sup> 15 U.S.C. § 1601 *et. seq.*

- G. "Credit history" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, or credit capacity that is used or expected to be used, or collected in whole or in part, for the purpose of determining personal lines insurance premiums or eligibility for coverage.
- H. "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.

**SECTION 2: SECURITY FREEZE<sup>12</sup>**

**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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>**

**Fortunately, most types of new account fraud are preventable by stopping, or "freezing" access to consumer credit files. In order for an identity thief to get credit, or to open an account for services in the name of a victim, the entity to whom the thief applies must check the consumer's credit file. 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. Consumers place the freeze, and then can grant access to their credit reports using a passcode, like an ATM PIN. Lacking the passcode, identity thieves cannot give access to their victims' credit reports, and find**

<sup>12</sup> The right to a security freeze should not be confused with trade line blocking or fraud alert rights. 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 credit report. But trade line blocking does not prevent the issuance of a consumer credit report; it only limits certain fraud-related information from being included in that report. Similarly, a fraud alert attached to a report does not prevent the report from being issued. A fraud alert merely conditions 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 bureau from issuing his or her report 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.

<sup>13</sup> 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](http://www.consumer.gov/idtheft/pdf/synovate_report.pdf).

<sup>14</sup> [http://www.consumer.gov/idtheft/pdf/synovate\\_report.pdf](http://www.consumer.gov/idtheft/pdf/synovate_report.pdf)

<sup>15</sup> Id.

that their applications for credit or services are denied as a result of the security freeze. Thus, the security freeze prevents thieves from opening new accounts in victims' names.

The model offers a security freeze that is free, easy to use, and available to all consumers. The proposed security freeze would not apply, however, to any person or entity with which consumers have existing accounts, nor to a limited number of other parties who may access the files for purposes not related to opening new accounts.

As a related protection, this model requires credit bureaus to notify consumers following new business requests (not from current creditors) for their credit reports or scores to assist consumers in detecting illegitimate access as well as attempted or actual fraud.

A security freeze should not be preempted by the federal Fair Credit Reporting Act. The federal law offers other, less useful tools, but does not address the issue of a security freeze. Federal law does require credit bureaus, upon the request of a consumer, (1) to put a fraud alert into the consumer's file to warn potential users of the report that new credit should not be extended without first verifying the identity of the credit applicant, and (2) to block the reporting of any information in a consumer's file that the consumer identifies as information resulting from an identity theft.<sup>16</sup> States are preempted from imposing requirements regarding the conduct required by these specific fraud alert and blocking provisions. These two provisions, however, do not establish any conduct with respect to freezing access to the entire report or score; as such states are free to enact this model law.

Security freezes have been adopted by 12 states, with some variations, as discussed below. This model's updated security freeze has been designed to reflect and improve upon the best practices emerging from recent state laws. The best form of security freeze borrows from the convenience of on-line banking, and enables the consumer to easily place and lift the freeze using the passcode with these changes taking effect almost immediately.<sup>17</sup> This model enables consumers to place and lift the freeze on-line, by telephone, or by fax. Many state freeze laws permit, but do not require, that these methods be offered. New Jersey and Texas go further; New Jersey requires that at least one of these methods be provided; and Texas specifies that consumers can request a lift, or "thaw" the freeze, by telephone. Making the process to use security freeze easier by providing for its electronic or telephone placement and removal will promote security freeze use and thus assist in the prevention of identity theft.

---

<sup>16</sup> The security freeze will provide better protection for consumers than the federal fraud alert and trade line blocking procedure. The Federal Trade Commission's rule creates a confusing, burdensome process for consumers to trigger this protection. Each credit bureau may establish different information and documentation to verify the fraud, and they may impose waiting periods totaling up to thirty-five days before they have to begin the blocking. *See*, Final Rule, Related Identity Theft Definitions, 16 C.F.R. pts. 603, 613, 614, available at: <http://www.ftc.gov/os/2004/10/041029idtheftdefsrn.pdf>.

<sup>17</sup> On-line banking demonstrates that it is technologically possible to develop a system to place and remove a security freeze on-line; telephone banking similarly shows the feasibility of telephone-managed security freezes.

According to the FTC, 43.3% of the identity theft complaints in 2004 involved situations other than the extension of credit that nonetheless involve the victim's credit report. Those covered include employment fraud, new phone and utility accounts, new insurance accounts, and property rental.<sup>18</sup> To stop these kinds of false new accounts, it is essential that the security freeze is not limited to those who are seeking to examine the consumer credit file for credit granting purposes.<sup>19</sup>

#### SIMILAR LEGISLATION:

Currently, California, Colorado, Connecticut, Illinois, Louisiana, Maine, New Jersey, Nevada, North Carolina, Texas, Vermont and Washington have passed versions of security freeze legislation.<sup>20</sup> Eight of these states make the security freeze available to all consumers, which maximizes its value as a preventive tool for consumers. Illinois, Texas and Vermont offer the freeze only to victims of identity theft. Washington state offers the freeze to identity theft victims, but uses a broad definition of identity theft victim, including persons who have received notice that the security of their personal information has been breached. In addition, the twelve state laws differ significantly in the cost of the freeze, and there is some variation in how the freeze is placed and lifted.

#### MODEL STATE LAW

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

- (1) "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.<sup>21</sup>

<sup>18</sup> This figure is calculated from data contained in the FTC's 2004 national report on identity theft complaints, page 10, available at: [http://www.consumer.gov/idtheft/pdf/clearinghouse\\_2004.pdf](http://www.consumer.gov/idtheft/pdf/clearinghouse_2004.pdf). The report indicates that 20.1% of the complaints involved new telephone or utility service, 13% related to employment fraud, 5% were new loans, 3.6% were new bank accounts, and 1.3% were property rental and new insurance accounts.

<sup>19</sup> By contrast, the same report notes that only 16.5% of complaints involved new credit cards.

<sup>20</sup> 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; 815 ILCS 505/2MM; La. Rev. Stat. Ann § 9.3571(H) to (Y); 2005 Me. Laws 243; NJ Pub. Law 2005, c. 226; 2005 Nev. Stat. 391; 2005 N.C. Sess. Laws 243; Tex. Bus. & Com. Code Ann. § 20.031 to 20.039; 9 Vt. Stat. Ann. § 2480a to 2480j; 2005 Wash. Laws 342.

<sup>21</sup> 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 credit report.

- (2) "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 credit report by:
  - a) making a request by mail,<sup>22</sup>
  - 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 electronic mail connection if such connection is made available by the agency. Credit reporting agencies shall make a secure electronic mail method of requesting a security freeze available within 180 days of this Act's effective date.
- 2) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than five business days after receiving a written or telephone request from the consumer or three business days after receiving a secure electronic mail request. 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 3 business days after receiving a written or telephone request from the consumer or one business day after receiving a secure electronic mail request. Within two years of this Act's effective date, a consumer reporting agency shall place a security freeze on a consumer's credit reporting agency no later than one business day after receiving a written or telephone request.<sup>23</sup>
- 3) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within five 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 credit 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 one business day after placing the freeze.
- 4) If the consumer wishes to allow his or her credit report 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,<sup>24</sup> or secure

<sup>22</sup> 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.

<sup>23</sup> This model uses graduated deadlines to move security freeze use toward the on-line banking model timelines. When a security freeze is on a consumer's credit report, a consumer who wants to open a new account in his or her own name must lift the freeze. While most new accounts can be planned for in a way that makes the five day deadline inconsequential, both consumer and creditor convenience may be enhanced by quick, efficient ways to lift the freeze. The gradual acceleration of the time frame for the consumer reporting agencies to process a request gives the agencies ample opportunity to determine how best to meet the deadlines.

<sup>24</sup> See fnt 21.

electronic mail, 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 credit report or the time period for which the report shall be available to users of the credit report.<sup>25</sup>

- 5) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to paragraph (4) of subsection (B) shall comply with the request no later than three business days after receiving the request. Within one year of this Act’s effective date, a consumer reporting agency shall honor such a request no later than one business day after receiving the request. Within two years of this Act’s effective date, a consumer reporting agency shall honor such a request made by electronic mail or by telephone within fifteen minutes of receiving the request.<sup>26</sup>
- 6) A consumer reporting agency shall develop procedures involving the use of telephone, fax, or, upon the consent of the consumer in the manner required by the Electronic Signatures in Global and National Commerce Act [E-Sign] for legally required notices, by the Internet, e-mail, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a credit report pursuant to paragraph (4) of subsection (B) in an expedited manner.<sup>27</sup>
- 7) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer’s credit report only in the following cases:
  - a) upon consumer request, pursuant to paragraph (4) or paragraph (10) of subsection (B);
  - b) 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 pursuant to this paragraph, the consumer reporting agency shall notify the

<sup>25</sup> 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. Ten states give consumers both options for managing their freeze. Louisiana and North Carolina allow the freeze to be thawed for specific time periods only.

<sup>26</sup> This model sets a two year timeline to reach the goal of 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. This element of the model law is based on the New Jersey law. New Jersey requires the Consumer Affairs Division of the Attorney General’s Office, in consultation with the Department of Banking and Insurance, to promulgate regulations to allow the freeze to thaw “as quickly as possible” and set a “goal” of thawing “within 15 minutes.” Those rules had not yet been issued as of October 2005.

<sup>27</sup> Eleven states have a provision similar to this one, except that it says the agency “may” develop rather than “shall” develop such procedures. New Jersey’s provision says “shall” develop, and Texas separately specifies that a consumer can thaw a freeze by telephone.

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 on which a security freeze is in effect, and this request is in connection with an application for credit or any other use, and the consumer does not allow his or her credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.
- 9) If a third party requests access to a consumer credit report on which a security freeze is in effect for the purpose of receiving, extending, or otherwise utilizing the credit therein, and not for the sole purpose of account review, the consumer credit report agency must notify the consumer that an attempt has been made to access the credit report.
- 10) A security freeze shall remain in place 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 within one business day after receiving such a request.
- 11) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.
- 12) 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.
- 13) The provisions of this section do not apply to the use of a consumer credit report by any of the following:
  - 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 person for the purposes of prescreening as defined by the federal Fair Credit Reporting Act.
  - h) any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed.
  - i) 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.
- 14) A consumer may not be charged for any security freeze services, including but not limited to the placement or lifting 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.<sup>28</sup>

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 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 credit report pursuant to [State law].

The security freeze will prohibit a consumer reporting agency from releasing any information in your 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 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 credit report or to temporarily authorize the release of your credit report 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:

---

<sup>28</sup> 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 effectively freeze his credit report, he 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, Illinois, Louisiana, Maine, Nevada, North Carolina, and Texas make all aspects of security freezes free to victims, and Louisiana also makes them free for the elderly. The best state law on security freeze fees overall is New Jersey, which makes placing a freeze free and caps the fee to thaw a freeze or replace a password at \$5.

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 credit report or the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request (By [date] the consumer reporting agency must temporarily lift the freeze within 15 minutes of receiving the request.)

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.”<sup>29</sup>

**Subsection D. Violations; Penalties.**

If a consumer reporting agency erroneously, whether by accident or design, violates the security freeze by releasing credit information 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 recover:
  - a) injunctive relief to prevent or restrain further violation of the security freeze, and/or

---

<sup>29</sup> 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. Colorado, New Jersey, North Carolina and Vermont require this notice be provided.

- b) a civil penalty in an amount not to exceed \$10,000 for each violation plus any damages available under other civil laws, and
  - c) reasonable expenses, court costs, investigative costs, and attorney's fees.
- 4) Each violation of the security freeze shall be counted as a separate incident for purposes of imposing penalties under this section.

### SECTION 3: PROTECTION FOR CREDIT HEADER INFORMATION

#### COMMENTARY

The term "credit header" refers to the personal identifying information in a consumer's credit file, including a consumer's name, address, telephone number, social security number, mother's maiden name, and birth date. The unrestricted use and sharing of this information can put consumers at serious risks if identity theft as well as other harms.<sup>30</sup> Unfortunately, with the exception of the consumer's age, this kind of sensitive, personal identifying information is not covered by the protections of the federal Fair Credit Reporting Act.<sup>31</sup> As a result, for years the credit bureaus routinely sold this information in bulk to direct marketers, private investigators, and others.

Currently, the federal Gramm-Leach-Bliley Act regulations do provide some protections for this data, but those restrictions are limited.<sup>32</sup> Under the rules, a credit bureau is free to sell consumers' credit header data if the financial institution that gave the bureau the information had first provided its customers with notice and the opportunity to opt out of the sharing.<sup>33</sup> In addition, any personal identifying information that the credit bureau itself collects directly from consumers also can be sold, subject to the bureau's privacy policy. Experian, for example, acquires consumers' personal information when validating consumers' identities for access to online credit reports and monitoring services. Experian's privacy policy suggests that this information is then shared with its affiliates unless the consumer opts-out, and for some of its products, the information is shared with non-affiliated third parties.<sup>34</sup>

**This model law closes these credit header loopholes by limiting the release of this data only to those individuals who would have a permissible purpose to**

<sup>30</sup> A New Hampshire woman, Amy Boyer, was stalked and killed by a man who purchased her social security number from an information broker that had access to the credit header data in Ms. Boyer's credit file. See, Kris Axtman, *When Criminals Get Help from the Web*, The Christian Science Monitor (May 9, 2000), available at <http://csmonitor.com/cgi-bin/durableRedirect.pl?durable/2000/05/09/text/p3s1.html>.

<sup>31</sup> *In re Trans Union Corp.* Docket No. 9255 (FTC, Feb. 10, 2000).

<sup>32</sup> *Privacy of Consumer Financial Information*, 16 C.F.R. pt. 313, available at <http://www.ftc.gov/os/2000/05/65fr33645.pdf>.

<sup>33</sup> Several studies have shown that consumers report great difficulty in understanding the terms of these privacy notices and the means for opting out. See, State AG Comments on the GLBA Information Sharing Study (May 3, 2002), available at [http://www.epic.org/privacy/financial/ag\\_glb\\_comments.html](http://www.epic.org/privacy/financial/ag_glb_comments.html).

<sup>34</sup> See, Credit Expert Privacy Policy, available at:

[https://www.creditexpert.com/CE\\_Site/Message.aspx?PageTypeID=Privacy](https://www.creditexpert.com/CE_Site/Message.aspx?PageTypeID=Privacy), and Scorecard Privacy Policy ("...we reserve the right to disclose all of the nonpublic personal information we collect."), available at <http://www.experian.com/privacy/scorecard.html>.

**obtain a consumer's credit report under the federal Fair Credit Reporting Act. States with their own state fair credit reporting act may want to limit the use to those with a permissible purpose under the state's law.**

**MODEL STATE LAW**

A consumer reporting agency may furnish information from a consumer's credit header only to those who have a permissible purpose to obtain the consumer's consumer report, under Section 604 of the federal Fair Credit Reporting Act, as codified at 15 U.S.C. § 1681(b), and that permissible purpose applies to the request for the credit header information.

**SECTION 4: 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.<sup>35</sup>**

**SIMILAR LEGISLATION**

**California, Connecticut, the District of Columbia, Illinois, Louisiana, Maryland, Michigan, North Carolina, Pennsylvania and Vermont all have state laws requiring that local police departments take police reports.<sup>36</sup> Many other states refer to the admissibility of police reports in identity theft prosecutions, but unfortunately do not have legislation requiring police departments to take such reports.<sup>37</sup>**

**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

<sup>35</sup> 15 U.S.C. §1681g.

<sup>36</sup> Cal. Penal Code § 530.6; 2003 Conn. Pub. Act. 03-156; D.C. Code Ann. § 22-3227.08; 720 Ill. Comp. Stat. § 5/16G-30; La. Stat. Ann. § 9:3568; Md. Code. Ann. Crim § 8-304.; MCLS § 780.754a; 2005 N.C. ALS 414; 18 Pa.C.S. § 4120e; Vt. Stat. Ann. tit. 9 § 2480k. *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>.

<sup>37</sup> In addition to allowing victims to file reports with their local police departments, states also may 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.

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 5: FACTUAL DECLARATION OF INNOCENCE AFTER IDENTITY THEFT**

**COMMENTARY**

**If a consumer has been a victim of an identity theft, he or she is at increased risk for further misuse of his or her personal information for unlawful purposes. Criminal identity theft occurs when a suspect in a criminal investigation identifies himself or herself using the identity of another, innocent person. As a result, a criminal record is created in the name of an innocent person. In such circumstances, a victim of identity theft must have the right to obtain a factual declaration of innocence from the courts in his or her state, and such declaration should be available through a statewide database that can be used to show others that the victim was not responsible for the crime.**

**This section of the model law establishes a procedure for criminal identity theft victims to obtain a factual declaration of innocence and a statewide criminal identity theft registry. This registry would be available via a toll-free number to the identity theft victim, criminal justice agencies and other individuals and agencies authorized by the victim to see the information. This provides a means for criminal identity theft victims to be able to demonstrate to authorities, employers, and others that he or she is not the individual who committed the crime(s). Carrying the declaration of factual innocence may prevent an innocent consumer from being arrested and jailed for someone else's crime.**

**SIMILAR LEGISLATION**

California, Colorado, Illinois, and North Carolina have strong laws regarding the factual declaration of innocence for victims of identity theft.<sup>38</sup> In Connecticut, the court may order the false information in public records resulting from identity theft be corrected.<sup>39</sup> California has established an Identity Theft Registry.<sup>40</sup>

**MODEL STATE LAW**

- A. A person who reasonably believes that he or she is the victim of identity theft may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move for an expedited judicial determination of his or her factual innocence, where the perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against the perpetrator in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the offense for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.
- B. After a court has issued a determination of factual innocence pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.
- C. Upon making a determination of factual innocence, the court must provide the consumer written documentation of such order.
- D. A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

<sup>38</sup> Cal. Penal Code § 530.6; 720; C.R.S. 16-5-103 Ill. Comp. Stat. § 5/16G-30; 2005 N.C. ALS 414.

<sup>39</sup> Conn. Gen. Stat. § 54-93a.

<sup>40</sup> Cal. Penal Code § 530.7; and *see*, *How to Use the California Identity Theft Registry*, Office of Privacy Protection, available at <http://www.privacy.ca.gov/sheets/cis8englsih.pdf>.

- E. The Supreme Court [of State, or as appropriate, Office of Court Administration, Judicial Council, etc] shall develop a form for use in issuing an order pursuant to this section.
- F. [Designated state agency] shall establish and maintain a data base of individuals who have been victims of identity theft and that have received determinations of factual innocence. [Designated state agency] shall provide a victim of identity theft or his or her authorized representative access to the data base in order to establish that the individual has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.
- G. [Designated state agency] shall establish and maintain a toll free number to provide access to information under subdivision (F).
- H. In order for a victim of identity theft to be included in the data base established pursuant to subdivision (F), he or she shall submit to the [designated state agency] a court order obtained pursuant to any provision of law, a full set of fingerprints, and any other information prescribed by the department.
- I. Upon receiving information pursuant to subdivision (H), the [designated state agency] shall verify the identity of the victim against any driver’s license or other identification record maintained by the Department of Motor Vehicles.
- J. This section shall be operative within 180 days of the passage of this Act.

**SECTION 6: CONSUMER-DRIVEN CREDIT MONITORING**

**COMMENTARY**

**The prevalence of identity theft and credit report errors requires consumers to be vigilant in monitoring their credit reports to detect fraud and inaccuracies. Federal law allows consumers one annual free credit report from each of the national credit bureaus. While this is an important consumer protection, checking a credit report once a year will not ensure early detection of fraud and mistakes. The major credit reporting agencies take advantage of this fact by marketing their expensive credit monitoring services to consumers as solutions. This marketing is inappropriate and may be deceptive.<sup>41</sup> Often the credit reporting agencies’ own lax procedures cause or facilitate the inaccuracies and fraud; they then sell services to facilitate the discovery of these errors. In addition, the credit reporting agencies have a statutory duty to take reasonable steps to ensure the maximum possible accuracy of consumers’ credit reports. As such, they**

---

<sup>41</sup> See, e.g., “Marketer of “Free Credit Reports” Settles FTC Charges: “Free” Reports Tied to Purchase of Other Products; Company to Provide Refunds to Consumers,” 16 August 2005, where Experian was ordered by the FTC to pay a \$950,000 fine plus consumer restitution for its marketing of its credit monitoring services, available at <http://www.ftc.gov/opa/2005/08/consumerinfo.htm> (last visited 6 November 2005).

should be providing consumers with regular, affordable access to their reports so that mistakes may be identified and corrected.

While the federal Fair Credit Reporting Act does preempt states from requiring more free access to consumer credit reports than provided by federal law, states retain the right to regulate the price of non-free credit reports.<sup>42</sup> This part of the model law allows consumers monthly access to their credit reports for a fee of up to two dollars per report, for up to twelve reports a year. Additional reports would cost eight dollars. This will allow consumers to engage in their own monthly monitoring. The model bill also would require credit bureaus to provide the requested reports to consumers within twenty-four hours of receiving a request.

**SIMILAR LEGISLATION**

**Credit monitoring services are a fairly new product, and to date no state has regulated their prices or developed an alternative to credit monitoring such as that provided in the model law.**

**MODEL STATE LAW**

Subsection A. Disclosures. Every consumer credit reporting agency shall, upon request from a consumer that is not covered by the free disclosures provided in 15 U.S.C. § 1681j subsections (a) through (d), clearly and accurately disclose to the consumer:

- 1) All information in the consumer's file at the time of the request, except that nothing in this paragraph shall be construed to require a consumer reporting agency to disclose to a consumer any information concerning credit scores or other risk scores or predictors that are governed by 15 U.S.C. § 1681g (f).
- 2) The sources of the information.
- 3) Identification of each person (including each end-user identified under 15 U.S.C. § 1681e) that procured a consumer report:
  - a) for employment purposes, during the 2-year period preceding the date on which the request is made; or
  - b) for any other purpose, during the 1-year period preceding the date on which the request is made.
- 4) An identification of a person under paragraph (3) of this subsection shall include
  - a) the name of the person or, if applicable, the trade name (written in full) under which such person conducts business; and
  - b) upon request of the consumer, the address and telephone number of the person.

---

<sup>42</sup> The FACT Act amendments to the federal FCRA grandfather in the existing free report on request laws of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and Vermont.

- 5) Paragraph (3) of this subsection does not apply if:
  - a) the end user is an agency or department of the United States Government that procures the report from the person for purposes of determining the eligibility of the consumer to whom the report relates to receive access or continued access to classified information (as defined in section 15 U.S.C. § 1681b (b)(4)(E)(i)); and
  - b) the head of the agency or department makes a written finding as prescribed under section 15 U.S.C. § 1681b (b)(4)(A).
- 6) The dates, original payees, and amounts of any checks upon which is based any adverse characterization of the consumer, included in the file at the time of the disclosure or which can be inferred from the file.
- 7) A record of all inquiries received by the agency during the 1-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer.
- 8) If the consumer requests the credit file and not the credit score, a statement that the consumer may request and obtain a credit score.

**Subsection B. Cost of Disclosure.** In the case of a request under subsection A, a consumer reporting agency may impose a reasonable charge on a consumer for making a report pursuant to this section, which charge:

- 1) shall not exceed \$2 for each of the first twelve requests from the consumer in a calendar year; and
- 2) shall not exceed \$8 for any additional request beyond the initial twelve requests from the consumer in a calendar year; and
- 3) shall be indicated to the consumer before making the disclosure.

**Subsection C. Format of Disclosure.** In the case of a request under subsection A, a consumer reporting agency must provide the consumer with an opportunity to access his or her report through all of the following means:

- 1) in writing;
- 2) in person, upon the appearance of the consumer at the place of business of the consumer reporting agency where disclosures are regularly provided, during normal business hours, and on reasonable notice;
- 3) by telephone, if the consumer has made a written request for disclosure;
- 4) by electronic means, if the agency offers electronic access for any other purpose; and
- 5) by any other reasonable means that is available from the agency.

**Subsection D. Timing of Disclosure.** A consumer reporting agency shall provide a report under subdivision A no later than:

- 1) twenty-four hours after the date on which the request is made, if the disclosure is made by electronic means, as requested under subsection C, paragraph (4); and
- 2) five days after the date on which the request is made, if the disclosure is made in writing, in person, by telephone or by any other reasonable means that is available from the agency.

**SECTION 7: PREVENTION OF AND PROTECTION FROM SECURITY BREACHES****COMMENTARY**

According to the Privacy Rights Clearinghouse, more than 80 data security breaches were reported in 2005, impacting an estimated 50 million plus consumers. These security breaches included financial institutions, data brokers, businesses, government agencies and universities. When the ChoicePoint scandal broke in February 2005, an estimated 35,000 consumers in California were notified, under what was then the only notice of breach law in the nation, that the security of their personal and financial information had been compromised.

In response, 38 state Attorneys General demanded that their state residents be informed of the ChoicePoint security breach as well. Since then, twenty states have passed notice of breach laws over the past year, taking the total number of states with notice of breach laws to twenty-one. Many of these bills contain elements of this model notice of breach language, while some contain other provisions or exceptions. The model notice of breach law is based on the premise that a company that has had a security breach should not get to decide whether or not to notify consumers about the breach.

Any entity that collects and maintains personal customer information as part of business operations should be required to establish security procedures to maintain the confidentiality and integrity of that data. 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 credit report and taking extra care when reviewing account statements.

**SIMILAR LEGISLATION**

Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Rhode Island, Tennessee, Texas, and Washington have enacted legislation requiring consumers to be notified when a breach of data security has occurred.<sup>43</sup>

**MODEL STATE LAW**

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

- 1) “Data Collector” 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

---

<sup>43</sup> Cal. Civil Code § 1798.80 – 1798.82.

purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personal information.<sup>44</sup>

- 2) “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 data collector. Good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector is not a breach of the security of the data, provided that the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure. Breach of the security of non-computerized data may include but is not limited to unauthorized photocopying, facsimiles, or other paper-based transmittal of documents.
- 3) “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 or debit card number, if circumstances exist wherein 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
  - 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 against the person whose information was compromised.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records, provided that such publicly available information has not been aggregated or consolidated into an electronic database or similar system by the governmental agency or by another person.<sup>45</sup>

**Subsection B. Notice of Breach.**

- 1) Except as provided in paragraph 2 of subsection B, any data collector 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,

<sup>44</sup> A minority of state notice of breach laws exclude financial institutions: Louisiana, Florida, Minnesota, Nevada, North Carolina, North Dakota and Tennessee. The Georgia, Maine, Montana and North Carolina laws do not include governmental agencies; while the Indiana law covers only government entities.

<sup>45</sup> 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.

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.<sup>46</sup>

- 2) 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.
- 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 would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, 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 was, or is reasonably believed to have been, acquired by an unauthorized person, including social security numbers, driver's license or State identification numbers and financial data;
  - b) a toll-free number--

---

<sup>46</sup> The model law covers all breaches of the security of sensitive personal information, while most state laws generally apply to information held in computerized form. In some states, business has sought exemptions so that consumers would not get notice of all security breaches. Some of the states that have adopted such exemptions have crafted them narrowly so that the business does not have unilateral power to decide whether or not to give the notice. For example, both Connecticut and Rhode Island require entities to conduct an appropriate investigation and consultation with relevant federal, state, and local law enforcement agencies. In Connecticut, notice is excused only when it has been reasonably determined that the breach will not likely result in harm and Rhode Island excuses notice unless it has been determined the breach poses a significant risk of identity theft. Florida’s law requires this same level of investigation and consultation with federal, state and local agencies and written documentation must be kept for 5 years. Other states have included an exception that nonetheless makes it clear that if the entity suffering the breach can’t predict the degree of risk, notice must be given. Thus, New Jersey requires a “thorough investigation that misuse of the information has not occurred and is not reasonably possible.” This determination must be made in writing and kept on file for 5 years. There are other variations as well.

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 impede a criminal investigation.

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 and on request and at no cost to such individual, 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.

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

Subsection D. Remedies.

- 1) Any individual injured by a violation of this section may institute a civil action to recover damages.
- 2) Any business that violates, proposes to violate, or has violated this section may be enjoined.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.<sup>47</sup>

---

<sup>47</sup> A number of states explicitly require their Attorneys General to enforce the notice of breach provisions including Arkansas, California, Connecticut, Delaware, Maine, Minnesota, Nevada, New York, North Dakota and Texas. Individuals have the right to seek and obtain personal damages as a result of a violation of the notice of breach law in Delaware, Tennessee and Washington. Louisiana, Maine, Rhode Island and Texas allow for monetary penalties for damages due to the entities' violations. Maine's law places a fine per violation and a fine for each day the entity is in violation of the law. Florida's law has penalties for notices which are not timely or if investigatory files are not documented and maintained. Nevada allows the data collector to commence an action against the person who unlawfully obtained data or unlawfully benefited from the breach

## SECTION 8: SOCIAL SECURITY NUMBER PROTECTION

## COMMENTARY

The widespread use of the social security number (SSN) as an identifier makes it relatively easy for thieves to use stolen or purchased SSNs of consumers to assume their identities and gain access to financial accounts and other sensitive information. As such, the use of consumers' SSNs for transactions, credit applications, or on drivers' licenses and other identification should be limited or prohibited. Social Security numbers are a key to a consumer's financial identity. No person should be required or coerced into providing a SSN unless it is essential to the transaction and no other identifier will suffice. Similarly, universities, health insurers and the military should not use SSNs as identifiers in information systems or on identification cards. The sale or public display of SSNs also should be restricted. Limiting the collection and approved uses of the SSN would help to reduce new cases of identity theft.

## SIMILAR LEGISLATION

Several states, including Arizona, California, Connecticut, Illinois, Indiana, New Jersey, North Carolina, and Texas have enacted legislation regarding the private sector use of SSNs that is similar to this model.<sup>48</sup> Arizona's statute also adds certain restrictions for state agencies and political subdivisions. Many other states have passed legislation limiting schools from using the SSN as a student identifier, and limiting the disclosure of SSNs on certain public records, but according to a recent General Account Office study, SSNs in state and local public records are less protected than SSNs appearing in federal public records.<sup>49</sup>

## MODEL STATE LAW

- A. Except as provided in subsection C, a person or entity, including a state or local agency, may not do any of the following:
- 1) Intentionally communicate or otherwise make available to the general public an individual's Social Security number.
  - 2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.
  - 3) 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, the number is essential to the transaction, and there is no other identifier that could reasonably be used.
  - 4) Require an individual to use his or her Social Security number to access an Internet Web site.

<sup>48</sup> Ariz. Rev. Stat. § 44-1373; Cal. Civil Code Ann. § 1798.85; Conn. Pub. Act. 03-156; 815 Ill. Comp. Stat. §505/2QQ; Ind. Code § 4-1-10.; 2005 N.C. ALS 414; NJ Pub. Law 2005. c. 226; Tex. Bus. & Commerce Code Ann. § 35.58.

<sup>49</sup> See, United States General Accounting Office, *GAO 05-59, Social Security Numbers: Governments Could Do More to Reduce the Display in Public Records and on Identity Cards*, (Nov. 2004), available at <http://www.gao.gov/new.items/d0559.pdf>.

- 5) Print an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed.
  - 6) Sell, lease, loan, trade, rent, or otherwise disclose an individual's Social Security number to a third party for any purpose without written consent to the disclosure from the individual.
  - 7) Refuse to do business with an individual because the individual will not consent to the receipt by such person of the social security account number of such individual, unless such person is expressly required under Federal law, in connection with doing business with an individual, to submit to the Federal Government such individual's social security account number.
- B. This section shall take effect no later than [date].<sup>50</sup>
- C. This section does not apply to documents that are recorded or required to be open to the public pursuant to [State codes]. This section does not apply to records that are required by statute, case law, or [State Supreme Court declaration], to be made available to the public by entities provided for in the [State Constitution].
- D. Any entity covered by this section shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this article are implemented on or before the dates specified in this section.
- E. Penalties for violations of this section.
- 1) A person who violates this section is responsible for the payment of a civil fine of not more than \$3,000.
  - 2) A person who knowingly violates this section is guilty of a misdemeanor punishable by imprisonment for not more than [days] or a fine of not more than \$5,000 or both.
  - 3) An individual may bring a civil action against a person who violates this section and may recover actual damages or \$5,000, whichever is greater, plus reasonable court costs and attorney's fees.

---

<sup>50</sup> If necessary, a reasonable phase-in timetable may be added to this legislation to implement Social Security number safety provisions. Such a timetable should:

- a) state a reasonable starting date by which all persons or entities, not including state or local agencies or providers described in below paragraph (c), must comply with subsection A;
- b) state a reasonable starting date, either the same date or a date not more than six months later, by which all state and local agencies must comply with subsection A;
- c) state a reasonable starting date, either the same date or a date not more than six months later, by which health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor, or the provision by any person or entity of administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only, must comply with subsection A.

## SECTION 9: BANNING CREDIT SCORING AND INSURANCE SCORING FOR USE IN INSURANCE DECISIONS

### COMMENTARY

Many insurance companies use consumers' credit information to influence their decisions about whether they will offer homeowners and automobile insurance to consumers and at what price. Using credit information for this purpose is unfair to consumers. Even if a consumer pays every insurance bill received on time and has never filed an insurance claim, a low credit score could result in significantly higher premiums, or even denial of coverage. Insurers should not be able to use credit scores derived from credit reports to deny consumers insurance or to place consumers in higher-risk (higher-cost) product pools. Insurance companies claim that there is a correlation between a consumer's score and the chance that he or she will file a future insurance claim. But they have kept their scoring formulas secret, preventing an independent, public review of the actuarial soundness of their claims. In addition, any correlation is insufficient to justify the use of insurance credit scoring. There are concerns that credit scoring may simply be a double counting of other risk factors that already are taken into consideration when setting insurance rates.<sup>51</sup> Scores also may be a proxy for rating factors that insurers are prohibited from using, such as race. This model law prohibits insurers from using information regarding a consumer's creditworthiness, credit standing, or credit capacity for the purpose of determining rates for insurance or eligibility for coverage.

### SIMILAR LEGISLATION

Many states have enacted legislation regarding credit scoring, but some of those that have looked at the issue in insurance have unfortunately elected to defer to the model law proposed by the National Conference of Insurance Legislators ("NCOIL"), an historically industry-friendly organization.<sup>52</sup> Alternatively, Maryland's homeowner insurance statute and Hawaii's auto insurance law are among the strongest in the country. In addition, Oregon has enacted a strong statute and corresponding regulations governing the use of insurance credit scores, and Michigan is considering prohibiting their use through legislation.<sup>53</sup>

The NCOIL model bill, unlike this model law, does not prevent the use of credit scores for insurance purposes. Instead, the NCOIL model authorizes this practice so long as the scoring is not the sole criterion used. Since scoring is never the sole factor used in underwriting or pricing insurance,

<sup>51</sup> See <http://www.cej-online.org/Simplified%20Credit%20Scoring%20Model.pdf>.

<sup>52</sup> According to a study by the Consumer Federation of America, at least 40 percent of the leadership of the National Conference of Insurance Legislators (NCOIL) has worked for or with the insurance industry and most of these NCOIL members have current business ties to the insurance industry. See, Consumer Federation of America, *NCOIL's Policy Positions Have Anti-Consumer Tilt*, June 2003, available at: <http://www.consumerfed.org/0709insurance.html>. For discussion of credit scoring issues, see Nelson & Cohen, *The Use of Credit Scoring in the Insurance Industry*, available at: <http://www.nldhlaw.com/CM/Articles/Articles53.asp>.

<sup>53</sup> Md. Code Ann. §27-501; Haw. Rev. Stat. § 431:10C-207; Or. Rev. Stat. Ann. § 746.661 to 746.663 and Or. Admin. R. 836-080-0425 (prohibits the cancellation or non-renewal based in whole or in part on credit information).

the bill offers consumers virtually no protection. Under the NCOIL legislation, insurers could continue to use credit scores, even though serious concerns have been raised about the actuarial soundness of the claim that credit history predicts consumer accident propensity, the inaccuracy of credit scores, and the disproportionate impact the practice has on low-income and minority consumers. In contrast, this model state law provides consumers with real protection by prohibiting the use of credit scoring or insurance scoring for rating and underwriting purposes.

#### MODEL STATE LAW

- A. With respect to private passenger automobile, residential property and other personal lines insurance, an insurer may not:
- 1) refuse to underwrite, cancel, refuse to renew a risk, or increase a renewal premium, based, in whole or in part, on the credit history of an applicant or insured; or
  - 2) rate a risk based, in whole or in part, on the credit history of an applicant or insured in any manner, including:
    - a) The provision or removal of a discount;
    - b) Assigning the insured or applicant to a rating tier; or
    - c) Placing an insured or applicant with an affiliated company; or
  - 3) require a particular payment plan based, in whole or in part, on the credit history of the insured or applicant.

#### SECTION 10: 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. Section 216 of the FACT Act and its implementing regulations require proper disposal only of that consumer information which is derived from 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 FACT Act 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 California, Georgia, Montana, Nevada, New Jersey, North Carolina, Texas, and Wisconsin have enacted legislation similar to this model.<sup>54</sup>

**MODEL STATE LAW**

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 any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, a name, signature, social security number, fingerprint and other biometric information, photograph or computerized image, physical characteristics or description, address, telephone number, passport number, driver's license or state identification care number, date of birth, medical information, bank account number, credit card number, debit card number, or any other financial information.
- 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.

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

---

<sup>54</sup> Cal. Civil Code Ann. § 1798.80 – 1798.84; Ga. Code Ann. § 10-15-1 – 10-15-2; Mont. Code. Ann. § 31-3-115; Nev. SB 347; 2005 N.C. ALS 414; NJ Pub. Law 2005. c. 226; Tex. Code. Ann. §48.102; 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.

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 11: 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.

## **Appendix:**

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

It also is available at:

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