Senate Counsel, Research, and Fiscal Analysis

G-17 State Capitol
75 Rev. Dr. Martin Luther King, Jr. Blvd.
St. Paul, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
Jo Anne Zoff Sellner
Director

Senate

State of Minnesota

S.F. No. 2002 - Omnibus Identity Theft Bill (as amended by SCS2002A-1)

Author: Senator Dan Sparks

Prepared by: Christopher B. Stang, Senate Counsel (651/296-0539)

Date: March 10, 2006

Section 1 gives a consumer the right to have a consumer reporting agency put a "security freeze" on the consumer's credit information. If a freeze is in place, the report may not be released to a third party without prior express authorization. Procedures are specified for placing the security freeze on the credit report. A consumer is allowed to lift the freeze under certain conditions by use of a unique personal identification number or password. No charge may be made to obtain the security freeze. Consumers must be notified of their rights to obtain a security freeze. Provides that an injured consumer can file a complaint with the Federal Trade Commission, the Minnesota Attorney General, or the Minnesota Department of Commerce. Allows a consumer to bring a civil action against a consumer reporting agency for a violation of this section. A consumer can obtain an injunction, damages, a civil penalty up to $10,000, expenses, court costs, investigative costs, and attorney fees.

Section 2 creates definitions of terms used in the sections 4 and 5 of the bill.

Section 3 is removed by the amendment.

Section 4 sets up a court process for identity theft victims to get a court determination that they are victims of identity theft. This is limited to situations in which the offender has been charged or convicted of a criminal offense under the victim's name. The Department of Public Safety would keep a database of court orders individuals could get under this section for individuals to access if they need to prove they have been victims of identity theft.

Section 5 allows a consumer not covered by the free disclosures required by federal law to get all information in the consumer's file except credit scores. Specified fees are allowed for requests for the information. Format and timing of disclosures are specified.

Section 6 is removed by the amendment.

Section 7 is removed by the amendment.

Section 8 requires businesses that operate in Minnesota or possess personal information about Minnesota residents to take reasonable measures to prevent unauthorized access to or use of the information after disposal of records. Provides examples of reasonable measures businesses might use without mandating any particular approach. Provides a $3,000 civil penalty for violations. Allows an individual harmed by a violation to bring a court action to enjoin future violations. Allows the individual to recover damages, costs, and attorney fees.

Section 9 is removed by the amendment.

A new **section 8** is added, which repeals exemptions for financial institutions and entities subject to HIPPA from legislation enacted last year regulating disclosure to persons affected by breach of a business entity's data security.

CBS:cs

AARP Minnesota

TESTIMONY OF HUBERT H. HUMPHREY III,
AARP MINNESOTA STATE PRESIDENT
BEFORE THE
SENATE COMMERCE COMMITTEE
SENATOR LINDA SCHEID, CHAIR

MARCH 15, 2006

Thank you for the opportunity to testify today in support of the **Clean Credit and Identity Theft Protection Act.** I am Skip Humphrey, State President of AARP Minnesota, representing more than 650,000 Minnesotans over the age of 50.

AARP would like to thank you, Senator Scheid, for holding this hearing on such an important topic not only to older Minnesotans but to Minnesotans of all ages.

In the Capitol Rotunda today, about 200 AARP members from around the state are gathering to showcase the need for legislation to protect consumers from identity theft. Another group of 250 members are planning to come next week to rally again on this same important issue. Obviously, our members care deeply about fighting identity theft.

AARP is pleased that this issue is being considered by your committee today. I would like to acknowledge the support we have from our bipartisan Senate authors, Chief Author Senator Dan Sparks, and Senators Metzen, Ruud, Koering and Chaudhary.

Identity theft is the taking of another's personal information -- such as a social security number, name or date of birth -- for the purpose of assuming the victim's identity to commit fraud. This crime affects people of all ages.

However, older people often are particularly attractive targets for identity thieves, experts say, because they tend to have accumulated relatively more savings and home equity, and have long credit histories.

At the end of 2004, AARP conducted a survey of 800 Minnesotans of all ages and we found that one quarter of Minnesota residents have been affected by the crime of identity theft, and eight in ten are concerned about becoming a victim of this growing crime. Almost all respondents (97%) said it is important for Minnesota to strengthen laws and regulations that protect consumers from identity theft.

Identity theft is a serious crime that is both widespread and costly. According to the Federal Trade Commission (FTC), ID theft costs businesses $50 billion per year, and consumers $5 billion per year nationally. An FTC survey released in January 2006, over 3,000 identity theft complaints were made to the ID Theft Clearinghouse from Minnesotans in 2005. While these numbers are alarming, it is important to note that many identity theft crimes currently go unreported.

People whose identities are stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing or automobiles, or even get arrested for crimes they did not commit.

In addition, the almost daily news reports about data breaches and mishandling of consumers' personal identifying information demonstrate how important it is to safeguard the personal information that not only identifies us, but also provides entrée into our most sensitive financial information. USA Today reported that in 2005, at least 130 reported breaches exposed more than 55 million people to potential identity theft.

Our top priorities in the legislation before you today are:

- Allowing consumers to place a security freeze on their credit report so that their information would only be shared with their consent;

- Strengthening last year's security breach notification law by removing the current exemptions granted to financial institutions and entities subject to HIPPA.

And let me say that AARP appreciates the work that this committee and the Legislature did last year. We do, however, urge you to close these two exemptions.

- Expanding access to credit reports so that consumers can monitor their reports on a monthly basis for a small fee; and, finally,

- Allowing victims to obtain a factual declaration of innocence to help clear their damaged credit rating.

Let me address further the issue of the security freeze provided by this legislation. A security freeze lets consumers stop identity thieves from getting credit in their names by locking access or "freezing" their credit files. This gives consumers the ability to control who sees the file for the purpose of opening new accounts. In most instances, businesses will not issue new credit to an applicant when the businesses cannot obtain credit information about the person.

It is important to note that if consumers freeze their credit files, it does not prevent them from obtaining new credit. Consumers can simply "thaw" the freeze by contacting the credit bureaus.

Over the last month, AARP has conducted three consumer fraud forums in partnership with the Minnesota Financial Crimes Task Force, the US Postal Inspection Service and the US Secret Service. These forums have helped educate nearly 500 older Minnesotans about how to avoid becoming a victim of identity theft and other scams. The audiences expressed overwhelming support for a security freeze.

Privacy is of considerable concern to AARP members, and our surveys show that most people do not believe that their personal information is being adequately protected. We are grateful that your committee has taken the time to consider this important issue and we welcome the opportunity to work with legislators and other stakeholders to pass legislation that will protect Minnesotans from the devastating crime of identity theft.

Thanks you again for the opportunity to testify here today.

AARP Minnesota

Clean Credit and Identity Theft Protection Act

AARP urges legislators to support House File 1943 and Senate File 2002 known as the *Clean Credit and Identity Theft Protection Act.*

1. Security Freeze

To help prevent identity theft, this legislation would require credit bureaus to notify consumers when a new request for their credit information is made. It will also allow individuals to "freeze" access to their credit reports until they give their approval. This tool is needed to combat "new account fraud." Allowing a convenient method to temporarily lift or "thaw" the freeze is provided in the bill.

2. Declaration of Innocence

This legislation gives victims of identity theft the right to obtain a "factual declaration of innocence" filed in court and with law enforcement agencies to alert authorities to the misuse of the consumer's identity or information.

3. Consumer-driven Credit Monitoring

Federal law now gives Minnesotans the right to one free credit report per year. This legislation would expand that access, and giving consumers the right to monthly access to their reports (for a minimum fee) so that mistakes may be identified and corrected.

4. Notification of Security Breaches

Any entity that collects and maintains personal customer information has a legal obligation to establish security procedures to maintain the confidentiality and integrity of that data. This legislation requires businesses to notify consumers when a breach in their security occurs. It will include financial institutions and health plans which are currently excluded from this notification requirement.

5. Destruction of Personal Records

This legislation requires businesses to properly dispose of records containing information that could be used to impersonate an individual.

AARP® Minnesota

Clean Credit and Identity Theft Protection Act
Questions and Answers

Q: What is identity theft?

A: 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.

Q: Didn't Congress preempt state laws for identity theft with the Fair and Accurate Credit Transactions Act (FACT Act)?

A: The 2003 FACT Act did preempt some types of state laws. Fortunately, the federal FACT Act did not interfere with most state authority to prevent and mitigate identity theft, to require personal data to be held securely, and to require that consumers be notified when there has been a breach in the security of their personal information. This law offers language in areas that states remain free to address.

Q: Didn't Minnesota legislators pass legislation in 2005 for customer notification of security breaches?

A: Yes, Minnesota was one of twenty states in 2005 to pass a security breach notification law. Our intent with our bill is to remove the two exemptions of financial institutions and entities subject to HIPAA. More that 80 data security breaches were reported nationwide in 2005, impacting an estimated 50 million consumers.

Q: How is a security freeze different than trade line blocking or a fraud alert?

A: The federal Fair Credit Reporting Act (FCRA) 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 some of the fraud-related information from being included in the report. A fraud alert only conditions the issuance of credit until certain identity verification procedures are complied with but does not prevent the credit bureau from selling or sharing the report with potential new creditors. A credit freeze allows any consumer the right to prevent the credit bureaus

from issuing his or her report for the purpose of issuing new credit or other new accounts. This bill freezes access to the report except for circumstances such as review of existing accounts and other limited purposes.

Q: What is new account fraud and what can a security freeze do to prevent it?

A: Identity thieves often use a victim's good credit history to open new accounts in the victim's name. Thieves fraudulently open a wide variety of accounts, including credit cards, loans, checking accounts, etc. They then fail to pay the bills, causing the new creditors to pursue the victim, and destroy the victim's 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.

Most new account fraud is preventable by "freezing" access to consumer credit files. In order for an id thief to get credit, or to open an account in the name of a victim, the entity to which 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.

Q: Is this bill updated with a security freeze thaw?

A: Yes. Our security freeze borrows from the convenience of on-line banking, and enables the consumer to easily place and lift the freeze using a pass code with these changes taking effect as soon as possible, but no more than 3 days. We want to work with legislators and other stakeholders to improve upon this provision with emerging best practices including the use of a fax and New Jersey's goal of 15 minutes.

Q: Which states have security freeze laws, and which consumers can implement a freeze?

A: Security freezes have been adopted by 12 states, with some variations. Currently, California, Colorado, Connecticut, Illinois, Louisiana, Maine, New Jersey, Nevada, North Carolina, Texas, Vermont and Washington have passed versions of security freeze legislation. Eight of these states make the security freeze available to all consumers, which maximizes its value as a preventive tool for consumers. The other four states offer the freeze only to victims of identity theft. AARP strongly supports this preventive protection for all consumers.

AARP Minnesota

Clean Credit and Identity Theft Protection Act

AARP urges legislators to support House File 1943 and Senate File 2002 known as the *Clean Credit and Identity Theft Protection Act.*

1. Security Freeze

To help prevent identity theft, this legislation would require credit bureaus to notify consumers when a new request for their credit information is made. It will also allow individuals to "freeze" access to their credit reports until they give their approval. This tool is needed to combat "new account fraud." Allowing a convenient method to temporarily lift or "thaw" the freeze is provided in the bill.

2. Declaration of Innocence

This legislation gives victims of identity theft the right to obtain a "factual declaration of innocence" filed in court and with law enforcement agencies to alert authorities to the misuse of the consumer's identity or information.

3. Consumer-driven Credit Monitoring

Federal law now gives Minnesotans the right to one free credit report per year. This legislation would expand that access, and giving consumers the right to monthly access to their reports (for a minimum fee) so that mistakes may be identified and corrected.

4. Notification of Security Breaches

Any entity that collects and maintains personal customer information has a legal obligation to establish security procedures to maintain the confidentiality and integrity of that data. This legislation requires businesses to notify consumers when a breach in their security occurs. It will include financial institutions and health plans which are currently excluded from this notification requirement.

5. Destruction of Personal Records

This legislation requires businesses to properly dispose of records containing information that could be used to impersonate an individual.

Members of the Minnesota Fair Information Practices Coalition

The Fair Information Practices Coalition wants to maintain a balance between the protection of individual information and the benefits of information sharing. The private sector voluntarily has taken aggressive steps to protect individual privacy. FIPC supports the businesses that adopt clear privacy statements, written in plain language, that are easily understood by the public. FIPC includes some 20 business organizations, representing hundreds of thousands of Minnesota workers. Among our members:

- Minnesota Business Partnership
- Minnesota Chamber of Commerce
- Minnesota Association of Realtors
- Minnesota Auto Dealers Association
- Independent Community Bankers of Minnesota
- Insurance Federation of Minnesota
- Minnesota Bankers Association
- Mortgage Association of Minnesota
- Minnesota Financial Services Association
- Direct Marketing Association
- Securities Industry Association
- Minnesota Telephone Association
- Minnesota Association of Mortgage Brokers, Inc.
- American Council of Life Insurers
- American Insurance Association
- Associated Credit Bureaus
- Investment Company Institute
- Minnesota Retailers Association
- Minnesota Grocers Association
- Greater Minneapolis Chamber of Commerce
- St. Paul Chamber of Commerce
- Twin West Chamber of Commerce
- Minnesota Credit Union Network
- Minnesota Credit Card Coalition

Bob Johnson

MINNESOTA FAIR INFORMATION PRACTICES COALITION

Relevant Points on Security Breach Disclosure Proposal

- Minnesota passed the ***Security Breach Disclosure Act*** in 2005, which provides significant consumer protections and rights to help prevent, manage and minimize negative results that might develop because of the breach. Twenty-two states have passed this type of law.

- Businesses in Minnesota strongly supported passage of this comprehensive, bi-partisan supported law.

- The Minnesota law includes a 'safe harbor', which properly recognizes that where a federal law requires notice of breach of security (i.e., Gramm-Leach-Bliley or GLB), then state law should not duplicate the federal law's requirements. Federal law should take precedence for uniformity and certainty for the many financial institutions covered that provide important financial services to consumers nationwide. Eleven of the 22 states that have passed security breach laws include a 'safe harbor' like Minnesota's law.

- Each institution's data security program is reviewed by its federal examining agency as part of regular safety and soundness examinations. The agency would note any data security deficiencies in its examination report, and the agency has full authority to take administrative action against the institution. These actions include fines and penalties of up to $1 million, 'cease and desist' orders and ultimately closing the institution.

- The federal GLB Act requires a risk-based approach that mandates assessing the nature/scope of an incident, the information accessed, notifying the primary federal examining agency and appropriate law enforcement agencies, taking steps to contain and control and notifying customers, when warranted.

- In 2005, Minnesota passed the NAIC Model Standards for Safeguarding Customer Information, required to be adopted by GLB, to generally require all licensed insurers and producers to implement information security programs to produce safeguards for nonpublic personal information, which must include administrative, technical and physical safeguards.

- State duplicative laws would add needless costs and complexities to financial institutions already complying with GLB, whose protections and notices consumers nationwide are accustomed to working with.

- The Federal Government continues to take an active oversight and review role in this area on behalf of consumers nationwide.

MINNESOTA FAIR INFORMATION PRACTICES COALITION

Relevant Points on Proposal To Regulate Use of SSNs

Background: Minnesota businesses use Social Security Numbers (SSNs) responsibly and for legitimate business purposes, such as identification and fraud prevention. The Federal Government requires, under the Patriot Act, that financial institutions collect SSNs to ensure customer identification. Unfortunately, there is no other widely accepted unique, national identifier, at this time. While identity theft is a serious issue, businesses, the Federal Government and states, like Minnesota, have taken appropriate steps to guard against the unauthorized disclosure and use of SSNs.

In 2005, Minnesota passed the ***Use of Social Security Numbers Act***, a significant law to help protect consumers from identity theft. The new law was patterned after a similar law in California and was strongly supported by Minnesota businesses.

The comprehensive protections included in the 2005 law include prohibiting business from:

- Publicly displaying a consumer's SSN.
- Printing the SSN on a card necessary for a consumer to obtain products or services.
- Requiring a consumer to use their SSN to access an Internet site.
- Requiring a consumer to transmit their SSN via the Internet unless the data is encrypted or the site uses a password or other security measures.
- Printing a consumer's SSN on mail unless another law requires it be sent.

The law recognizes that in the absence of an acceptable alternative, businesses that currently use SSNs may not be able to provide services such as paying claims or processing/servicing loans without SSNs. Developing and implementing an alternative system does not add any additional consumer protections and would be costly and disruptive for consumers.

Continual Use Essential; Adds Consumer Safeguards

- To strike an appropriate balance, the Legislature determined that businesses currently and continually using SSNs could continue so long as consumers are given notice of those practices and the opportunity to opt-out at no charge. The law also includes an anti-coercion provision that prevents businesses from denying services to consumers who request to opt-out of SSN use.

- The exception for continuous use is essential to allow businesses to deliver service with minimal disruption while limiting practices that could lead to identity theft.

- Minnesota has already adopted the toughest standard in the nation. Further action at this time will impede the delivery of financial and other services without providing any additional meaningful protections.

Senate Counsel, Research, and Fiscal Analysis

G-17 State Capitol
75 Rev. Dr. Martin Luther King, Jr. Blvd.
St. Paul, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
Jo Anne Zoff Sellner
Director

Senate

State of Minnesota

S.F. No. 2145 - Credit Report Blocking

Author: Senator Mike McGinn

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MK

Date: March 14, 2006

The bill allows consumers, upon submission of a valid police report, to permanently block the reporting of any information on their credit report, which the consumer alleges is the result of identity theft. The bill requires credit reporting agencies to promptly notify the furnisher of the information that the information has been blocked and permits unblocking of the information only if: there is material misrepresentation of fact, or fraud, by the consumer; the consumer agrees the information was blocked in error; or if the consumer knowingly obtained goods, services, or money as a result of the blocked transaction.

A1 amended. Adopted as amended.
Recommend to pass, as amended
and re-referred to Judiciary.

Senators Sparks, Koering, Metzen, Ruud and Chaudhary introduced--

S.F. No. 2002: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; authorizing a consumer to place a security freeze on the consumer's credit report; providing notice of this right; providing protections against identity theft; providing Social Security number protections; providing credit monitoring; providing for the adequate destruction of personal records; providing civil and criminal penalties; proposing coding for new law in Minnesota Statutes, chapters 13C; 325E.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [13C.05] [SECURITY FREEZE ON CONSUMER CREDIT REPORTS.]

Subdivision 1. [DEFINITIONS.] For the purposes of this section, the following terms have the meanings given them:

(1) "security freeze" means a notice, at the request of the consumer and subject to certain exceptions, prohibiting 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; and

(2) "reviewing the account" or "account review" includes activities related to account maintenance, monitoring, credit

line increases, and upgrades and enhancements.

Subd. 2. [TIMING; COVERED ENTITIES; COST.] (a) A consumer may elect to place a security freeze on a credit report by:

(1) making a request by certified mail;

(2) making a request by telephone by providing certain personal identification; or

(3) making a request directly to the consumer reporting agency through a secure electronic mail connection if the connection is made available by the agency.

(b) 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.

(c) 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 the consumer's credit for a specific party or period of time.

(d) If the consumer wishes to allow the consumer's credit report to be accessed for a specific party or period of time while a freeze is in place, the consumer shall contact the consumer reporting agency via telephone, certified mail, or secure electronic mail; request that the freeze be temporarily lifted; and provide the following:

(1) proper identification;

(2) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (c); and

(3) the proper information regarding the third party who is to receive the credit report or the time period for which the report must be available to users of the credit report.

(e) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report

pursuant to paragraph (d) shall comply with the request no later than three business days after receiving the request.

(f) A consumer reporting agency may develop procedures involving the use of telephone or fax, or upon the consent of the consumer in the manner required by the Electronic Signatures in Global and National Commerce Act, United States Code, title 15, section 7001 et seq., 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 (d) in an expedited manner.

(g) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:

(1) upon consumer request, pursuant to paragraph (d) or (j); or

(2) if the freeze was 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 consumer in writing five business days before removing the freeze on the consumer's credit report.

(h) 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 the consumer's credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

(i) 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 using the credit in the report, and not for the sole purpose of account review, the consumer reporting agency must notify the consumer that an attempt has been made to access the credit report.

(j) Except as otherwise provided in paragraph (g), clause

(2), 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:

(1) proper identification; and

(2) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (c).

(k) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

(l) 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.

(m) This section does not apply to the use of a consumer credit report by any of the following:

(1) 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;

(2) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under paragraph (d) for purposes of facilitating the extension of credit or other permissible use;

(3) any person acting pursuant to a court order, warrant, or subpoena;

(4) a state or local agency which administers a program for establishing and enforcing child support obligations;

(5) the Department of Health or its agents or assigns acting to investigate fraud;

(6) the Department of Revenue or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders to fulfill any of its other statutory

responsibilities;

(7) a person for the purpose of prescreening as defined by the federal Fair Credit Reporting Act;

(8) any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed; and

(9) any person or entity for the purpose of providing a consumer with a copy of the consumer's credit report upon the consumer's request.

(n) 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 may be charged no more than $5 only if the consumer fails to retain the original personal identification number given to the the consumer by the agency, but the consumer may not be charged for a onetime reissue of the same or a new personal identification number. The consumer may be charged no more than $5 for subsequent instances of loss of the personal identification number.

Subd. 3. [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, the following notice must be included:

"Minnesota 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 .....

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 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:

(1) the unique personal identification number or password provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(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.

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 credit, you should understand that the procedures involved in lifting a security freeze may slow your own application for credit. You should plan ahead and lift a freeze, either completely if you are shopping around, or specifically for a certain creditor, a few days before actually applying for new credit.

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.

Subd. 4. [VIOLATIONS; PENALTIES.] (a) 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, the state attorney general, and the Department of Commerce; and

(3) in a civil action against the consumer reporting agency recover:

(i) injunctive relief to prevent or restrain further violation of the security freeze;

(ii) a civil penalty in an amount not to exceed $10,000 for each violation plus any damages available under other civil laws; and

(iii) reasonable expenses, court costs, investigative costs, and attorney fees.

(b) Each violation of the security freeze must be counted as a separate incident for purposes of imposing penalties under this section.

Sec. 2. [325E.60] [DEFINITIONS.]

Subdivision 1. [SCOPE.] For the purposes of sections 325E.60 to 325E.62, the terms in subdivisions 2 to 10 have the meanings given.

Subd. 2. [PERSON.] "Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

Subd. 3. [CONSUMER.] "Consumer" means an individual.

Subd. 4. [CONSUMER REPORTING AGENCY.] "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, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

Subd. 5. [CONSUMER REPORT; CREDIT REPORT.] "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 creditworthiness, 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 sections 325E.60 to 325E.62 authorizes the use of credit evaluations or credit scoring in the underwriting of personal lines of property or casualty insurance;

(2) employment purposes; or

(3) any other purpose authorized under United States Code, title 15, section 1681b.

Subd. 6. [IDENTITY THEFT.] "Identity theft" means theft, fraud, or attempted theft or fraud committed using any identifying information of another person.

Subd. 7. [NONPUBLIC PERSONAL INFORMATION.] "Nonpublic personal information" has the meaning given the term under section 509(4) of the Gramm-Leach-Bliley Act, which defines "nonpublic personal information" to mean personally identifiable financial information that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. It also includes any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information.

Subd. 8. [CREDIT CARD.] "Credit card" has the same meaning as in section 103 of the Truth in Lending Act.

Subd. 9. [DEBIT CARD.] "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.

Subd. 10. [CREDIT HISTORY.] "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.

Sec. 3. [325E.61] [POLICE REPORT REGARDING IDENTITY THEFT.]

Subdivision 1. [RIGHT TO FILE.] A person who has learned or reasonably suspects that he or she has been the victim of identity theft may contact the local law enforcement agency that has jurisdiction over his or her actual residence. The local law enforcement agency shall make a written 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.

Subd. 2. [CONSEQUENCES.] 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.

Sec. 4. [325E.62] [FACTUAL DECLARATION OF INNOCENCE AFTER IDENTITY THEFT.]

Subdivision 1. [JUDICIAL DETERMINATION.] 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.

Subd. 2. [COURT ORDER.] 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.

Subd. 3. [DOCUMENTATION.] Upon making a determination of factual innocence, the court must provide the consumer written documentation of such order.

Subd. 4. [VACATING DETERMINATION.] 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.

Subd. 5. [FORM.] The Supreme Court shall develop a form

for use in issuing an order pursuant to this section.

Subd. 6. [DATABASE.] The Department of Public Safety shall establish and maintain a database of individuals who have been victims of identity theft and that have received determinations of factual innocence. The Department of Public Safety shall provide a victim of identity theft or his or her authorized representative access to the database in order to establish that the individual has been a victim of identity theft. Access to the database shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.

Sec. 5. [325E.63] [CONSUMER-DRIVEN CREDIT MONITORING.]

Subdivision 1. [DISCLOSURES.] Every consumer credit reporting agency shall, upon request from a consumer that is not covered by the free disclosures provided in United States Code, title 15, section 1681j, subsections (a) to (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 subdivision requires a consumer reporting agency to disclose to a consumer any information concerning credit scores or other risk scores or predictors that are governed by United States Code, title 15, section 1681g(f);

(2) the sources of the information;

(3) identification of each person, including each end-user identified under United States Code, title 15, section 1681e, that procured a consumer report:

(i) for employment purposes, during the two-year period preceding the date on which the request is made; or

(ii) for any purpose, during the one-year period preceding the date on which the request is made;

(4) an identification of a person under clause (3) shall include:

(i) the name of the person or, if applicable, the trade name (written in full) under which such person conducts business; and

(ii) upon request of the consumer, the address and telephone number of the person;

(5) clause (3) does not apply if:

(i) 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 United States Code, title 15, section 1681b(b)(4)(E)(i)); and

(ii) the head of the agency or department makes a written finding as prescribed under United States Code, title 15, section 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 one-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.

Subd. 2. [COST OF DISCLOSURE.] In the case of a request under subdivision 1, a consumer reporting agency may impose a reasonable charge on a consumer for making a disclosure pursuant to this section, which charge must:

(1) not exceed $3 for each of the first 12 requests from the consumer in a calendar year;

(2) not exceed $8 for any additional request beyond the initial 12 requests from the consumer in a calendar year; and

(3) be indicated to the consumer before making the disclosure.

Subd. 3. [FORMAT OF DISCLOSURE.] In the case of a request under subdivision 1, a consumer reporting agency must provide the consumer with an opportunity to access his or her report

through 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;

(5) by any other reasonable means that is available from the agency.

Subd. 4. [TIMING OF DISCLOSURE.] A consumer reporting agency shall provide a consumer report under subdivision 1 no later than:

(1) 24 hours after the date on which the request is made, if the disclosure is made by electronic means, as requested under subdivision 3, clause (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.

Sec. 6. [325E.64] [PREVENTION OF AND PROTECTION FROM SECURITY BREACHES.]

Subdivision 1. [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 purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information;

(2) "breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, and confidentiality, or integrity of personal

information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for a legitimate purpose of the agency is not a breach of the security of the system data, provided that the personal information is not used for a purpose unrelated to the agency or subject to further unauthorized disclosure. Breach of the security of noncomputerized 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 first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social Security number;

(ii) driver's license number or state identification card number;

(iii) 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;

(iv) account passwords or personal identification numbers (PINs) or other access codes;

(v) any of items (i) to (iv) when not in connection with the individual's first name or first initial and last name, 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.

Subd. 2. [NOTICE OF BREACH.] (a) Except as provided in paragraph (b), any data collector that owns or uses personal information in any form, whether computerized, paper, or otherwise, that includes personal information concerning a Minnesota resident shall notify the resident that there has been a breach of the security that data following discovery or notification of the breach, without regard for whether or not

the data has or has not been accessed by an unauthorized third party for legal or illegal purposes. The disclosure notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (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.

(b) The notification required by this section may be delayed if a law enforcement agency determines that the notification may impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(c) For purposes of this section, "notice" to consumers may be provided by one of the following methods:

(1) written notice;

(2) 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 United States Code, title 15, section 7001;

(3) substitute notice, if the agency demonstrates that the cost of providing notice would exceed $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 consists of all of the following:

(i) e-mail notice when the agency has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the agency's Web site page, if the agency maintains one; and

(iii) notification to major statewide media.

Sec. 7. [325E.65] [SOCIAL SECURITY NUMBER PROTECTION.]

Subdivision 1. [PROHIBITIONS.] Except as provided in subdivision 2, 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;

(4) require an individual to use his or her Social Security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site;

(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; or

(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.

Subd. 2. [NONAPPLICATION.] This section does not apply to documents that are recorded or required to be open to the public pursuant to chapter 13. This section does not apply to records that are required by statute, case law, or court order to be made available to the public by entities provided for in the Minnesota Constitution.

Subd. 3. [HEALTH CARE SERVICES.] In the case of a 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, this section shall become operative no later than July 1, 20...

Subd. 4. [COOPERATION.] 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 section are implemented on or before the dates specified in this

section.

Subd. 5. [PENALTIES FOR VIOLATIONS OF THIS SECTION.] (a) A person who violates this section is subject to a civil penalty of not more than $3,000.

(b) 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.

(c) An individual may bring a civil action against a person who violates this act and may recover actual damages or $5,000, whichever is greater, plus reasonable court costs and attorney fees.

Sec. 8. [325E.66] [ADEQUATE DESTRUCTION OF PERSONAL RECORDS.]

Subdivision 1. [DEFINITIONS.] For the purposes of this section, the following terms shall have the meanings given them:

(a) "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.

(b) "Dispose" includes:

(1) the discarding or abandonment of records containing personal information; and

(2) the sale, donation, discarding, or transfer of any medium, including computer equipment, or computer media, containing records of personal information, or other nonpaper media upon which records of personal information is stored, or other equipment for nonpaper storage of information.

(c) "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, photograph or computerized image, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, date of birth, medical information, bank account number, credit card number, debit card number, or any other financial information.

(d) "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.

Subd. 2. [DISPOSAL OF RECORDS CONTAINING PERSONAL INFORMATION.] Any business that conducts business in Minnesota and any business that maintains or otherwise possesses personal information of residents of Minnesota must take all reasonable measures to protect against unauthorized access to or use of the information in connection with, or after its disposal. Such reasonable measures must include, but may not be limited to:

(1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed;

(2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper 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; and

(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 clauses (1) and (2).

Subd. 3. [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.

Subd. 4. [PENALTIES AND CIVIL LIABILITY.] (a) Any person or business that violates this section is subject to a civil penalty of not more than $3,000.

(b) Any individual aggrieved by a violation may bring a civil action in district court to enjoin further violations and to recover actual damages, costs, and reasonable attorney fees.

Sec. 9. [SEVERABILITY.]

The provisions of this act are severable. If any phrase, clause, sentence, provision, or section is declared to be invalid or is preempted by federal law or regulation, the remaining provisions of the act remain valid.

adopted

Senator Sparks moves to amend S.F. No. 2002 as follows:

Page 7, line 19, delete "325E.60" and insert "325E.65"

Page 7, line 21, delete "325E.60 to 325E.62" and insert "325E.65 to 325E.67"

Page 8, delete lines 20 to 36

Page 9, delete lines 1 to 29

Page 9, line 30, delete "325E.62" and insert "325E.66"

Page 11, line 12, delete "325E.63" and insert "325E.67"

Pages 13 to 17, delete sections 6 and 7

Page 17, line 12, delete "325E.66" and insert "325E.68"

Page 19, delete section 9

Page 19, after line 30, insert:

"Sec. 8. **REPEALER.**

Minnesota Statutes 2005 Supplement, section 325E.61, subdivision 4, is repealed."

Renumber the sections in sequence and correct the internal references

Amend the title accordingly

Sen. Kiscaden delete

Deleted lines 11, 12 + 13

Withdrawn

Senator Michel ..... moves to amend S.F. No. 2002 as follows:

Page 7, after line 18, insert:

"Sec. 2. Minnesota Statutes 2005 Supplement, section 325E.61, subdivision 4, is amended to read:

Subd. 4. **Exemption.** This section does not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3)~~, and to entities subject to the federal privacy and security regulations adopted under the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191~~."

Amend the title accordingly

Section 1 S.F. 2002
amend title accordingly

Senators McGinn, Jungbauer and Koering introduced--

S.F. No. 2145: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; providing a procedure to block the reporting of information in a consumer credit report in cases of identity theft; proposing coding for new law in Minnesota Statutes, chapter 13C.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [13C.032] [IDENTITY THEFT; CREDIT BLOCKS.]

(a) If a consumer submits to a credit reporting agency a copy of a valid police report, or a valid investigative report made by an investigator with peace officer status, the consumer credit reporting agency shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of section 609.527 so that the information cannot be reported. The consumer credit reporting agency shall promptly notify the furnisher of the information that the information has been blocked. Furnishers of information and consumer credit reporting agencies shall ensure that information is unblocked only upon a preponderance of the evidence establishing the facts required under paragraph (b), clause (1), (2), or (3).

(b) The permanently blocked information must be unblocked only if:

(1) the information was blocked due to a material misrepresentation of fact by the consumer or fraud;

(2) the consumer agrees that the blocked information, or

portions of the blocked information, were blocked in error; or

(3) the consumer knowingly obtained possession of goods, services, or money as a result of the blocked transaction or transactions or the consumer should have known that he or she obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

(c) If blocked information is unblocked pursuant to this subdivision, the consumer must be promptly notified. The prior presence of the blocked information in the consumer credit reporting agency's file on the consumer is not evidence of whether the consumer knew or should have known that he or she obtained possession of any goods, services, or money. For the purposes of this subdivision, fraud may be demonstrated by circumstantial evidence. In unblocking information pursuant to this subdivision, furnishers and consumer credit reporting agencies are subject to their respective requirements pursuant to this chapter regarding the completeness and accuracy of information.

A-1 adopted

incorporate into the body of SF 2002
amend title accordingly

Senators McGinn, Jungbauer and Koering introduced--

S.F. No. 2144: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; regulating credit card offers and solicitations; requiring address corrections; proposing coding for new law in Minnesota Statutes, chapter 325G.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [325G.052] [CREDIT CARD OFFERS AND SOLICITATIONS; ADDRESS VERIFICATIONS.]

(a) A credit card issuer that mails an offer or solicitation to receive a credit card and, in response, receives a completed application for a credit card that lists an address that is different from the address on the offer or solicitation shall verify the change of address ~~by contacting the person to whom the solicitation or offer was mailed.~~ "before issuing a credit card"

(b) Notwithstanding any other provision of law, a person to whom an offer or solicitation to receive a credit card is made is not liable for the unauthorized use of a credit card issued in response to that offer or solicitation if the credit card issuer does not verify the change of address pursuant to paragraph (a) before the issuance of the credit card, unless the credit card issuer proves that this person actually incurred the charge on the credit card.

(c) When a credit card issuer receives a written or oral request for a change of the cardholder's billing address and then receives a written or oral request for an additional credit

card within ten days after the requested address change, the credit card issuer shall not mail the requested additional credit card to the new address or, alternatively, activate the requested additional credit card, unless the credit card issuer has verified the change of address.

Adopted

Senator Sparks moves to amend S.F. No. 2144 as follows:

Page 1, line 13, delete everything after "address"

Page 1, delete line 14 and insert "before issuing a credit card."

Senate Counsel, Research, and Fiscal Analysis

G-17 State Capitol
75 Rev. Dr. Martin Luther King, Jr. Blvd.
St. Paul, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
Jo Anne Zoff Sellner
Director

Senate

State of Minnesota

S.F. No. 2193 - Credit Report Security Alert

Author: Senator Michael J. Jungbauer

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MK

Date: March 14, 2006

The bill allows consumers to place a security alert in their credit report in cases of suspected identity theft. The security alert would notify recipients of the report of possible fraudulent use of the consumer's identity and requires recipients of the report to take additional steps to verify the consumer's identity prior to the extension of credit in that consumer's name. The bill also requires each credit reporting agency to establish a 24 hour toll-free telephone number to accept security alert requests from consumers.

MSG:cs

no action

Senators Jungbauer, Wergin and Nienow introduced--

S.F. No. 2193: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; authorizing a consumer to place a security alert on a consumer credit report; proposing coding for new law in Minnesota Statutes, chapter 13C.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [13C.032] [SECURITY ALERT.]

(a) A consumer may elect to place a security alert in the consumer's credit report by making a request in writing or by telephone to a consumer credit reporting agency. "Security alert" means a notice placed in a consumer's credit report, at the request of the consumer, that notifies a recipient of the credit report that the consumer's identity may have been used without the consumer's consent to fraudulently obtain goods or services in the consumer's name.

(b) A consumer credit reporting agency shall notify each person requesting consumer credit information with respect to a consumer of the existence of a security alert in the credit report of that consumer, regardless of whether a full credit report, credit score, or summary report is requested.

(c) Each consumer credit reporting agency shall maintain a toll-free telephone number to accept security alert requests from consumers 24 hours a day, seven days a week.

(d) The toll-free telephone number must be included in any written disclosure by a consumer credit reporting agency to a

consumer and must be printed in a clear and conspicuous manner.

(e) A consumer credit reporting agency shall place a security alert on a consumer's credit report no later than five business days after receiving a request from the consumer.

(f) The security alert shall remain in place for at least 90 days, and a consumer shall have the right to request a renewal of the security alert.

(g) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, or with the purchase, lease, or rental of goods or non-credit-related services and who receives notification of a security alert pursuant to paragraph (a) may not lend money, extend credit, or complete the purchase, lease, or rental of goods or non-credit-related services without taking reasonable steps to verify the consumer's identity, in order to ensure that the application for an extension of credit or for the purchase, lease, or rental of goods or non-credit-related services is not the result of identity theft. If the consumer has placed a statement with the security alert in the consumer's file requesting that identity be verified by calling a specified telephone number, any person who receives that statement with the security alert in a consumer's file pursuant to paragraph (a) shall take reasonable steps to verify the identity of the consumer by contacting the consumer using the specified telephone number before lending money, extending credit, or completing the purchase, lease, or rental of goods or non-credit-related services. If a person uses a consumer credit report to facilitate the extension of credit or for another permissible purpose on behalf of the subsidiary, affiliate, agent, assignee, or prospective assignee, that person may verify a consumer's identity under this section in lieu of the subsidiary, affiliate, agent, assignee, or prospective assignee.

(h) For purposes of this section, "extension of credit" does not include an increase in the dollar limit of an existing open-end credit plan, as defined in Regulation Z issued by the Board of Governors of the Federal Reserve System, Code of

Federal Regulations, title 12, section 226.2, or any change to, or review of, an existing credit account.

(i) A consumer credit reporting agency shall notify each consumer who has requested that a security alert be placed on the consumer's credit report of the expiration date of the alert.

(j) A consumer credit reporting agency that recklessly, willfully, or intentionally fails to place a security alert pursuant to this section is liable for a penalty in an amount of up to $2,500 and reasonable attorney fees.

Senate Counsel, Research, and Fiscal Analysis

G-17 State Capitol
75 Rev. Dr. Martin Luther King, Jr. Blvd.
St. Paul, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
Jo Anne Zoff Sellner
Director

Senate

State of Minnesota

S.F. No. 2194 - Credit Card Solicitations

Author: Senator Michael J. Jungbauer

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MG

Date: March 14, 2006

The bill allows consumers to have their names removed from any list that a consumer credit reporting agency furnishes for credit card solicitations by notifying the credit reporting agency by telephone or in writing.

MSG:cs

no action

Senators Jungbauer and Nienow introduced--

S.F. No. 2194: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; regulating consumer credit reporting agencies; providing a process to remove a consumer's name from credit card solicitation lists; proposing coding for new law in Minnesota Statutes, chapter 13C.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [13C.032] [CREDIT CARD SOLICITATION LISTS; CONSUMER ELECTION TO REMOVE NAME.]

A consumer may elect to have the consumer's name removed from any list that a consumer credit reporting agency furnishes for credit card solicitations by notifying the consumer credit reporting agency by telephone or in writing. The election is effective for a minimum of two years, unless otherwise specified by the consumer.

Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

Not heard on 3/15/06

S.F. No. 2960 - Credit Report Security Freeze

Author: Senator Satveer Chaudhary

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MG

Date: March 14, 2006

The bill allows consumers to place a security freeze on their credit report to prohibit credit reporting agencies from releasing the consumer's credit report or any information derived from it without the express authorization of the consumer.

Subdivision 1 provides definitions.

Subdivision 2 establishes: the means by which a consumer may request and remove a credit report security freeze; the manner in which a consumer may grant specific access to their credit report; the conditions under which a credit reporting agency may remove a security freeze; the manner in which a security freeze is dealt with by third parties requesting access to a consumer's credit report; and instances in which the security freeze does not apply to a consumer's credit report.

Subdivision 3 requires notice to consumers of their right to obtain a credit report security freeze.

Subdivision 4 subjects persons violating the provisions of a security freeze to penalties and remedies under the additional duties of the Minnesota Attorney General.

MSG:cs

Not heard
on 3/15/06

Senators Chaudhary, Skoglund, Sparks, Limmer and Scheid introduced–

S.F. No. 2960: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; permitting consumers to "freeze" their credit reports as a matter of security; proposing coding for new law in Minnesota Statutes, chapter 13C.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[13C.05] CONSUMER SECURITY FREEZE.**

Subdivision 1. **Definitions.** For the purposes of this section, the following terms have the following meanings:

(a) "Consumer" means an individual.

(b) "Consumer reporting agency" means any person, 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.

(c) "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 United States Code, title 15, section 1681(b).

(d) "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.

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

Subd. 2. **Security freeze; timing, covered entities, cost.** (a) A consumer may place a security freeze on his or her credit report by:

(1) making a request by first class United States mail;

(2) making a request by telephone by providing certain personal identification; or

(3) making a request directly to the consumer reporting agency through a secure electronic mail connection, which connection shall be made available by the agency.

(b) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than three business days after receiving a request pursuant to paragraph (a).

(c) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within three business days of placing the freeze and at the same time shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit report for a specific party or specific period of time, or when permanently lifting the freeze.

(d) If the consumer wishes to allow his or her credit report to be accessed by a specific party or for a specific period of time while a freeze is in place, the consumer shall contact the consumer reporting agency via telephone, first class United States mail, or secure electronic mail, with a request that the freeze be temporarily lifted, and provide the following:

(1) proper identification;

(2) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (c); and

(3) the proper information regarding the third party who is to receive the credit report or the time period for which the report is available to users of the credit report.

(e) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to paragraph (d) shall comply with

the request as quickly as possible, but in no event later than three business days after receiving the request.

(f) 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 federal Electronic Signatures in Global and National Commerce Act, United States Code, title 15, section 7001, et seq., for legally required notices, by the Internet, electronic 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 (d) in an expedited manner.

(g) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:

(1) upon consumer request, pursuant to paragraph (d) or (j); or

(2) 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 consumer in writing five business days before removing the freeze on the consumer's credit report.

(h) 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.

(i) 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 using the credit in it, and not for the sole purpose of account review, the consumer credit reporting agency must notify the consumer that an attempt has been made to access the credit report.

(j) A security freeze remains in place until the consumer requests that the security freeze be removed. A consumer reporting agency shall remove a security freeze as quickly as possible, but in no event later than three business days after receipt of a request for removal from a consumer who provides both of the following:

(1) proper identification; and

(2) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (c).

(k) A consumer reporting agency shall require proper identification of the person making a request to remove a security freeze.

(l) 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.

(m) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

(1) 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;

(2) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subdivision 2, paragraph (d), for purposes of facilitating the extension of credit or other permissible use;

(3) any person acting pursuant to a court order, warrant, or subpoena;

(4) a state or local agency which administers a program for establishing and enforcing child support obligations;

(5) the Department of Health or its agents or assigns acting to investigate fraud;

(6) the Department of Revenue 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;

(7) any person administering a credit file monitoring subscription service to which the consumer has subscribed; or

(8) any person for the purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.

(n) A consumer may not be charged for any services related to the security freeze, except that a consumer reporting agency may charge a consumer a fee of no more than $5 to reissue a personal identification number or password issued pursuant to paragraph (c).

Subd. 3. **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, United States Code, title 15, section 1681(g), the following notice must be included:

"Minnesota 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 Minnesota 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 three business days 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 for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number or password provided by the consumer reporting agency.

(2) Proper identification to verify your identity.

(3) The proper information regarding the third party or parties who are to receive the 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 as quickly as possible, but no later than three business days after 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. You should lift the freeze at least three business days before applying for a new account."

Subd. 4. **Penalties and remedies.** A person violating this section is subject to the penalties and remedies in section 8.31.

Senator Scheid from the Committee on Commerce, to which was referred

S.F. No. 2002: A bill for an act relating to consumer protection; authorizing a consumer to place a security freeze on the consumer's credit report; providing notice of this right; providing protections against identity theft; providing Social Security number protections; providing credit monitoring; providing for the adequate destruction of personal records; providing civil and criminal penalties; proposing coding for new law in Minnesota Statutes, chapters 13C; 325E.

Reports the same back with the recommendation that the bill be amended as follows:

Page 1, before line 12, insert:

"Section 1. **[13C.032] IDENTITY THEFT; CREDIT BLOCKS.**

(a) If a consumer submits to a credit reporting agency a copy of a valid police report, or a valid investigative report made by an investigator with peace officer status, the consumer credit reporting agency shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of section 609.527 so that the information cannot be reported. The consumer credit reporting agency shall promptly notify the furnisher of the information that the information has been blocked. Furnishers of information and consumer credit reporting agencies shall ensure that information is unblocked only upon a preponderance of the evidence establishing the facts required under paragraph (b), clause (1), (2), or (3).

(b) The permanently blocked information must be unblocked only if:

(1) the information was blocked due to a material misrepresentation of fact by the consumer or fraud;

(2) the consumer agrees that the blocked information, or portions of the blocked information, were blocked in error; or

(3) the consumer knowingly obtained possession of goods, services, or money as a result of the blocked transaction or transactions or the consumer should have known that he or she obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

(c) If blocked information is unblocked pursuant to this subdivision, the consumer must be promptly notified. The prior presence of the blocked information in the consumer credit reporting agency's file on the consumer is not evidence of whether the consumer knew or should have known that he or she obtained possession of any goods, services, or money. For the purposes of this subdivision, fraud may be demonstrated by circumstantial evidence. In unblocking information pursuant to this subdivision, furnishers and consumer credit reporting agencies are subject to their respective requirements pursuant to this chapter regarding the completeness and accuracy of information."

Page 7, line 19, delete "325E.60" and insert "325E.65"

Page 7, line 21, delete "325E.60 to 325E.62" and insert "325E.65 to 325E.67" and delete "10" and insert "6"

Page 8, line 11, delete "325E.60 to 325E.62" and insert "325E.65 to 325E.67"

Page 8, delete lines 20 to 36

Page 9, delete lines 1 to 29

Page 9, line 30, delete "325E.62" and insert "325E.66"

Page 11, line 12, delete "325E.63" and insert "325E.67"

Pages 13 to 17, delete sections 6 and 7

Page 17, line 12, delete "325E.66" and insert "325E.68"

Page 19, delete section 9 and insert:

"Sec. 7. **[325G.052] CREDIT CARD OFFERS AND SOLICITATIONS; ADDRESS VERIFICATIONS.**

(a) A credit card issuer that mails an offer or solicitation to receive a credit card and, in response, receives a completed application for a credit card that lists an address that is different from the address on the offer or solicitation shall verify the change of address before issuing a credit card.

(b) Notwithstanding any other provision of law, a person to whom an offer or solicitation to receive a credit card is made is not liable for the unauthorized use of a credit card issued in response to that offer or solicitation if the credit card issuer does not verify the change of address before issuing a credit card.

(c) When a credit card issuer receives a written or oral request for a change of the cardholder's billing address and then receives a written or oral request for an additional credit card within ten days after the requested address change, the credit card issuer shall not mail the requested additional credit card to the new address or, alternatively, activate the requested additional credit card, unless the credit card issuer has verified the change of address."

Renumber the sections in sequence

Amend the title accordingly

And when so amended the bill do pass and be re-referred to the Committee on Judiciary. Amendments adopted. Report adopted.

Linda Scheid .....
(Committee Chair)

March 15, 2006 .....
(Date of Committee recommendation)