Consumers Union
Nonprofit Publisher of Consumer Reports

July 7, 2006

Senator Ken Hansen
Joint Economic Affairs Interim Committee
P.O. Box 686
Harlem, MT 59526-0686

RE: Comments on the Interim Committee draft on the security freeze and related issues

Dear Senator Hansen,

Consumers Union, the non-profit independent publisher of *Consumer Reports* ®, appreciates the opportunity to work with Montana policymakers to develop a strong legislative proposal for a security freeze law. Montana consumers need a simple, low cost tool to stop the opening of new accounts by thieves. That need is illustrated by the May 2006 Department of Veterans Affairs security breach. The VA breach and the continuing security breaches with private companies, universities, government, and other entities have resulted in over 80 million consumers having their sensitive personal data compromised in less than two years. A security freeze law would give each Montana consumer a choice to stop the conversion of stolen data into new accounts for credit, goods or services in the consumer's name.

A strong security freeze law would give every Montana consumer a low cost, easy-to-use way to restrict access to his or her consumer reporting file when that consumer is not seeking use it. Consumers Union has endorsed the Montana Attorney General's security freeze proposal, which permits only a $3 one time administrative fee and a lost PIN fee. The draft now before the Interim Committee will not serve Montana consumers unless the fees are reduced. If the Attorney General's one time, $3 fee proposal is not adopted, we respectfully suggest that the Interim Committee cap all fees at $5 per step and also eliminate fees for persons receiving a notice of security breach and for permanently removing the freeze.

This letter discusses the important fee issues in sections 1- 4. Section 5 discusses the other open issues in the security freeze draft on a section by section basis. Section 6 describes decisions made by the Interim Committee and reflected in the draft with which Consumers Union is in strong agreement. Section 7 comments on the other anti-identity theft bill drafts before the Interim Committee.

1. The $10 per step fee permitted by the draft is much too high.

We respectfully suggest that this security freeze proposal cannot serve Montana consumers well unless it provides for lower fees, such as the one-time $3 fee proposed by the Attorney General, or the $5 fee found in several recent state laws.

The draft authorizes a $10 fee for each step of the process, other than for ID theft victims and possibly persons who have received a notice of a security breach. Consumers Union asks the Interim Committee to

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

reconsider the $10 fee level. Fees that can be charged by each CRA and for each step in the freeze/lift/removal process impose a high burden on individuals and families because the fee must be paid multiple times. For example, the $10 fee in section 10 of the draft would actually cost a two adult household who places the freeze and lifts it just once in the first year a total of $80, plus another $60 if they later permanently remove their freezes. (2 adults x 3 CRAs x $10 to place, + 2 adults x $10 for one lift = $80). This is too much for Montanans to pay to protect themselves from creditors and service providers who extend credit and services to identity thieves.

The security freeze has spread rapidly, with laws enacted in 25 states. The expanded scope of state freeze laws should bring down the cost of providing the freeze in any one state. Some state legislators are insisting on lower fees for their constituents.

These states have enacted laws with lower fees than the $10 found in the Committee's working draft:

State	Fee to place	Fee to lift	Fee to remove	Seniors	Victims
Minnesota	$5	$5	$5	--	no fee
New York	$0 first time then $5	$5	$5	--	no fee
New Jersey	$0	$5	$5		no fee
Colorado	$0 first time	$10/$12	$10	no fees to place	
Oklahoma	no fees to place or remove for persons age 65 or older, and no fees for victims				
Louisiana	no fee by placing CRA for persons age 62 and over.				

Another approach, taken by Delaware, combines the placement and removal fee into a too-high $20 fee to place and disallows all fees for lifting or removing the freeze.

A CRA has several means of generating revenue using the consumer reporting file while the freeze is in effect. During the freeze, a CRA can continue to sell access to the file to existing creditors and for other uses which are exempt from the freeze. A CRA can continue to use the information in that file for prescreening, which is permitted under federal law unless the consumer has taken the trouble to opt out. The CRA also can continue to sell credit monitoring or a credit score to the consumer, generating additional fee revenue.

Consumers Union respectfully suggests that there is no reason for Montana consumers to pay more for the security freeze than the residents of Minnesota, New York and New Jersey.

Recommended change: The per step fee permitted by section 10 should be reduced to $5.

2. There should be no fees for consumers who have received a notice of security breach.

The draft poses the issue of whether fees should be eliminated for consumers who have been notified of a security breach involving the consumer's own personal information. We respectfully urge that those fees be eliminated. Consumers whose information has been breached may have a special need for the security freeze, because the theft of their information creates a heightened risk of identity theft. In addition, a large security breach may generate new revenue for the CRAs, because some consumers whose information is compromised in a security breach will choose to buy credit monitoring, at their own expense or perhaps at the expense of the entity who had the breach. For example, before the missing VA laptop was found, the VA announced that it would pay for credit monitoring for veterans at an expected cost of $160 million. Thus, security breaches can produce increased revenue for CRAs, which could offset a fee waiver for those consumers who wish to respond to a notice of breach by placing a security freeze.

Consumers who feel a special need for a security freeze after being notified that their own sensitive personal information was compromised in a security breach should not face high fees to place that freeze. Both the consumer and creditors will be better off if that consumer places a freeze which deprives any thief holding the consumers' personal information from using that information to open new accounts. The consumer will be better off because he or she won't have to resolve the mess created by a false account. The creditor or seller of goods will be better off because it won't get stuck with uncollectible debt incurred by the thief.

Recommended change: Include the bolded language in section 10(2) to exempt consumers who have been notified of a security breach of their own personal information from security freeze fees.

3. There should be no fee to remove a security freeze.

Nearly all of the state laws permit a fee to remove the security freeze, but such a fee is bad public policy. Consumers will know about a fee to place a security freeze, because they have to pay it to begin the process. A fee to remove the freeze is much more likely to be an unpleasant surprise. Since removing the freeze actually simplifies handling of the consumer file for the CRA, why should the consumer have to pay for the removal? One state, Louisiana, does not permit a fee to remove the freeze.

Recommended change: Section 10(1) should be amended to delete "removal of a freeze," thus eliminating the authorization for a fee to remove the freeze.

4. Consumers who make a complaint to law enforcement but cannot get a copy of the police report should not be penalized.

The staff chart indicates that the working group recommended that consumers be given a way to prove their status as identity theft victims when they can't get a local police department to issue a report. We agree. Consumers Union supports the Committee's efforts in another draft bill to require that a police report always be taken in the home jurisdiction of an ID theft victim. However, victims' advocates in other states tell us that consumers continue to report difficulties in getting a police report even when state law requires that a report be taken. Many state freeze laws address this by allowing a consumer to show victim status using a copy of a police report, investigative report *or* a copy of a complaint the consumer has filed with a law enforcement agency. Illinois, Maine, Nevada, and North Carolina, for example, take this approach. Texas also defines a victim to include a person who has filed a complaint with a law enforcement agency.

Recommended change: Include the bolded language in section 10(2).

5. Section by section discussion of other issues that will affect the usefulness of the freeze.

The draft and accompanying chart present a number of important issues - in bolded language in the draft - for further discussion. The resolution of these issues will affect the usability and value of the Montana security freeze.

Section 2(2): There should be a shorter time, such as one or three days, for electronic placement.

Section 2(2) presents the issue of a quicker time for placement of the security freeze if placed electronically. The comments to the draft raise the issue of a quicker time for placement of the security freeze when placed electronically. Consumers Union believes that the 24 hour time for placement which the bill provides elsewhere for identity theft victims is also the appropriate time for placement by electronic means. One state, Minnesota, requires placement of the security freeze within three business days even when it is placed by mail. New York requires that all requested freezes be placed within three business days by January 1, 2009.

Recommended language: Change "5" to "3" in section 3(1), or add a new subsection 2(3) such as: "When the freeze is requested by electronic means as provided in section 2(2), it shall be placed within 24 hours."

Section 3(3): The PIN should be sent within five business days.

The time to send the confirmation is also the time to send the PIN. The confirmation provides the consumer with peace of mind, and the PIN lets the consumer use his or her own credit. The Attorney General suggested five business days, and the CDIA suggested ten business days. Delays in the mail could make the actual waiting time longer, since this is only the time for sending the confirmation and PIN, not the time for receipt. Consumer reporting agencies are already required by New Jersey law to confirm and send the PIN within five business days. There is no reason for Montana consumers to have to wait twice as long for a PIN as people in New Jersey.

Recommendation: Section 3(3) should select the 5 business day period.

Section 3(3): The scope of what would be authorized by adding "similar device" is unknown.

The CDIA has proposed that the freeze be lifted using a PIN, password, or "similar device." Consumers Union is not aware of any state that has adopted the "similar device" approach. The CDIA should clarify what methods would be permitted by this unproven change. It is essential that no device be permitted that is less secure than a PIN or password. Questions based on information in a consumer's credit file may not be sufficient if those questions draw upon information that may also be contained in publicly available records (such as prior addresses) or upon information held by third parties that may be subject to a data security breach.

Recommendation: This change is not recommended based on current information.

Section 4(1): If a CRA designates a point of contact for lifting the freeze, it must be required to designate contact points for *each* allowable method of contacting that CRA.

If each CRA is permitted to designate the point of contact for requests to lift a freeze, then they must be required to designate a point of contact for *each* allowable method of lifting the freeze. Section 4(1) permits the use of mail, phone, or a secure electronic method to lift the freeze. Section 4(3)(a) requires that the CRA designate the contact address, phone number, fax number *or* appropriate electronic access address. If section 4(1) is changed to require that the consumer use the point of contact designated by the CRA, then 4(1) and 4(3) should be amended to make it clear that the CRA must designate a point of contact for each allowable method of contact. If a CRA in fact accepts phone or fax requests, for example, then it should not be permitted to designate only a mailing address.

Recommended change: If the bolded language in section 4(1) is included, change it to: "using one point of contact selected by the consumer from points of contact designated by the consumer reporting agency for regular or certified mail, telephone, or a secure electronic method..." A conforming change in section 4(3)(a) could read: "designate an address for each of the following methods which is allowed for use in requesting a lift of the security freeze: mail address, phone number, fax number, or appropriate electronic access address..."

The issue of a designated point of contact also arises in section 7, but since mail is the only method provided to remove the freeze, there is no issue of the designation cutting off other allowable methods to remove the freeze.

Section 4(2): The bill should provide an earlier time to lift the freeze than three business days.

The bolded language at section 4(2) mandates that CRAs comply with a request to lift the freeze no later than 3 business days after receiving the request "or at the earliest time generally provided to consumers in another state, whichever is earlier." It would give Montana consumers the convenience of a faster lift when CRAs provide a faster lift to consumers in other states. Faster lifts must be in place for consumers elsewhere by September 1, 2008 under a Utah law, and by Jan. 31, 2009 under a just-signed Delaware law.

Reducing the time to lift the freeze to the shorter time available to consumers in other states will benefit both businesses and consumers. Businesses will be assured that they can access a consumer's credit file sooner to complete a transaction and consumers will be able to open new accounts more quickly.

Recommendation: Include the bolded language at section 4(2) for a faster time to lift the freeze when faster times are provided to consumers in another state.

Section 4(3)(c): Consumers should receive a method to lift the freeze without the delays inherent in mailing a request.

Section 4(3)(c) includes bolded language for lifting of the freeze by phone, fax or electronic media in addition to mailed requests. This language would require at least one non-mail method to lift the freeze, but it would let each CRA decide which non-mail method to provide. This will not be a new burden on CRAs. Texas law already permits consumers to lift a security freeze by phone. Utah law requires both phone and a secure electronic method starting Sept. 1, 2008. New Jersey law requires procedures for phone, fax, Internet or electronic media. CRAs could comply with this element of the Montana bill by

offering the phone method they already offer to comply with Texas law, or by offering an electronic method that they also use to satisfy the requirements of another state's law.

Non-mail methods are feasible – TransUnion's posted instructions tell consumers how to lift the freeze by phone. See:
http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/securityFreeze.xml.

We also offer a technical drafting suggestion about how section 4(3)(c) should be worded.
The language requiring that there be procedures for one or more non-mail methods doesn't expressly state that the purpose of those non-mail methods is to use in requesting a lift of the freeze. This could be clarified by adding: "to request a temporary lift of the security freeze." In addition, the reference to the requirements of the federal E-Sign Act may not be needed in this section. E-Sign requirements are vitally important when the company communicates with the consumer, who might not be expecting to receive e-mail communications if the E-Sign consent process hasn't been used. E-Sign requirements should not be necessary where, as under this subsection, the consumer would be the one initiating an electronic communication with the CRA.

Recommendation: Include the bolded language at section 4(3)(c) requiring at least one non-mail method to request a lift of the freeze, and modify that language to refer to the purpose of those methods and to delete the reference to E-Sign.

Section 5: There should be notice to the consumer before the freeze is involuntarily removed.

Section 5 offers language sought by the Attorney General that would require notice to the consumer five business days before removal of a freeze. The drafting notes suggest that no other state has this requirement, but in fact New Jersey law and the very recent Delaware law both require five business days notice before removal not at the request of the consumer, and the Minnesota freeze law requires prior notice of three business days. In addition, many states require notice prior to the involuntary removal, without specifying a time period. These states include California, Colorado, Florida, Illinois, Oklahoma, Kentucky, New Hampshire, New York, North Carolina, Louisiana, and Utah.

Recommendation: Include the bolded language in section 5, but clarify that the prior notice is only required when the freeze is removed under subsection (1)(b).

Section 6: The proposed language to notify consumers of attempts to access a frozen consumer file is valuable.

Section 6(2) contains language proposed by the Attorney General requiring the CRA to notify the consumer when an attempt to access the consumer report or score is made for credit purposes other than account review. This notice could tell consumers that someone is attempting to impersonate them. Though this is unique, it would be valuable for consumers, since it might allow consumers to learn that someone is impersonating them when the thief is first shut out of the credit file, before the thief moves on to other forms of identity theft, such as attempting to open a fake bank account.

Recommendation: Include the bolded language in section 6.

Section 7: The point of contact issue is discussed above, under section 4.

Section 8: The choices for the notice depend on the policy choices made in sections 3 ("device") and 4 (faster lifting with electronic method).

Section 9(7): The effect of the change in the prescreening language is not clear.

The change sought by the CDIA in exemption 9(7) does not appear to have a substantive effect. CDIA should explain what it believes this change would do.

Section 9(12): The insurer exemption creates some risk for consumers.

Section 9(12) exempts persons regulated under Title 33, that is, insurers. While we do not believe that an insurer exemption is necessary, we acknowledge that states are making varying policy choices on this question. An exemption for all insurers and insurance agents, regardless of their purpose in seeking access to the consumer reporting file, is too broad. For example, if an insurer decided to go into the consumer reporting business, no exemption should apply.

Recommended change: If section 9(12) is retained, add: "for purposes of engaging in the business of insurance which are otherwise permitted by law." This would restrict an insurer exemption to insurance uses, and leave to other law the issue of when an insurer is permitted to use credit information in insurance pricing.

Section 9(14): The screening database exemption works if it does not exempt databases used both for screening and for other purposes.

The exemption for screening databases needs the words "solely" and "entirely" to avoid creating a loophole for non-screening databases. The recent Florida law, HB 37, section 501.005(12)(j), contains an exemption for screening databases identical to the bolded language in section 9(14) with the inclusion of the limiting words "solely" and "entirely." With these words included, the databases which are exempt are those which are composed "entirely" of screening information and are used "solely" for one or more of the stated screening purposes. Here is a link to the text of the Florida law: http://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h0037er.doc&DocumentType=Bill&BillNumber=0037&Session=2006. Including the words "entirely" and "solely" has the important effect of ensuring that the exemption applies only to databases used for certain kinds of non-credit, non-new accounts screening, and that exemption does not apply to all uses of a database which is used for both credit and similar accounts and also for tenant, employment, criminal or fraud pattern screening. An exemption for a multi-purpose database, rather than just for particular types of uses of such a database, would be a very significant loophole in the protection offered by a security freeze.

Recommendation: Include exemption 9(14) only if the bracketed words "solely" and "entirely" are included. The policy issues raised by the "personal loss history" language are similar to the issues in the coverage or non-coverage of insurance uses of consumer reporting information.

Section 10: The fees should be reduced.

The important issue of fees is discussed at the start of this letter. Consumers Union urges the Interim Committee to revisit its May 2006 decision on fees and to reduce the fee to $5 per step, or less. We also ask the Committee to: 1) adopt the Attorney General's proposal that there be no fee on persons who have received notice of a security breach involving their personal information, 2) eliminate fees to permanently remove the freeze, and 3) permit ID theft victims to avoid the fee by showing that they have made a complaint to a law enforcement agency even if they cannot get a police report.

Section 14: July 2007 is an appropriate effective date.

Twenty five states have now enacted security freeze laws. The CRAs can comply with the Montana law by using the security freeze platform that they have already developed for other states. Nothing in this bill draft or these recommendations would require significant CRA retooling. Montana consumers should not have to wait any longer than necessary for this right. A delayed effective date is not needed. If the CDIA were able to show that one or two specific parts of the Montana law require a longer lead time, only those parts should be considered for a delayed effective date.

Recommendation: Set the effective date for July 2007.

6. The security freeze draft makes several important choices that will aid consumers.

We are in strong agreement with certain decisions of the Interim Committee. These choices include the use of regular mail and an electronic method to place the freeze, the avoidance of a limitation on the freeze to credit purposes only, the requirement for 24 hour freeze placement for ID theft victims and the choice for the temporary lift for a specific party or a specific period of time. These issues will be discussed briefly below.

The Interim Committee made the right decision to allow consumers to choose regular mail to place the freeze and to choose electronic placement after a short post-enactment delay. Allowing consumers to choose regular mail or an electronic method avoids the extra time, cost and inconvenience of certified mail, and an electronic method may have the additional advantage of leading to faster placement of the freeze. This can be important when the consumer has recently learned of a data security breach, had a wallet stolen, or experienced a theft of personal financial records.

We also support the element of the draft which avoids restricting the freeze to purposes related to the extension of credit. New accounts for goods and services, such as cell phone accounts opened by thieves, can affect a consumer's credit score and economic opportunities. In some states, a restriction to credit purposes has been sought by insurers or by companies maintaining non-credit screening databases. This bill draft already contains an exclusion for Montana insurers in section 9, exemption 12. Section 9, exemption 14 would address screening databases if they are used solely for specific purposes such as employment screening, tenant screening, criminal record information, or fraud prevention or detection. There is simply no need for, and there would be much harm from, a restriction to credit purposes.

We also are in strong agreement with the decisions to allow consumers to choose the form of the temporary lift for a specific party or for a specific period of time and to provide faster placement of the freeze to ID

theft victims. These decisions will give consumers more ability to restrict access to their consumer reporting files, a key purpose of the security freeze.

7. Comments on other anti-ID theft and data privacy drafts before the Interim Committee.

Government collection of SSNs (LCzzzz): Consumers Union supports the efforts of the Interim Committee to develop a package of anti-identity theft measures. The measure addressing government collection and disclosure of Social Security numbers, for example, will help to ensure that government does not collect these numbers when they are not needed, and that government protects the confidentiality of SSNs when it does collect them. In evaluating this draft, the Interim Committee may wish to add a "legitimate purposes" restriction to the sharing of SSNs between government agencies. Section 1(2)(c)(i)(C) of that draft permits a government agency to disclose an SSN to any other state or federal government entity. That subsection does not require that the disclosure under that subsection from one government entity to another government entity be "for a legitimate purpose" or "for a purpose otherwise permitted under this Act." Adding such a requirement would strengthen the measure.

Assistance to victims of ID theft (LC 8877): Consumers Union supports many provisions of the draft "Act providing assistance to victims of identity theft." We are not certain that consumers will benefit from being required to offer two forms of identification when making a report to a police agency. With child identity theft, it may be difficult to produce two forms of ID, since children below middle school age often do not yet have a picture ID. However, we defer to Montana law enforcement agencies, including the Attorney General, for their views on whether this is needed and whether the bill should clarify how this requirement will be met when a guardian complains on behalf of a minor child.

We strongly support the right in section 2 of this draft to request and receive one free copy of a data broker file per calendar year. This language is simple and balanced. Consumers get access once a year, but the consumer who wants to see the file must ask for it and access may be restricted in certain specific circumstances.

The improvements to the ID theft passport program in section 3 should be valuable, although the provision that accepting the passport is at the discretion of each law enforcement agency (and each creditor) may reduce its usefulness. The expungement process and the right to a refund of extra insurance premiums paid due to someone else's criminal record will be useful.

Offsite government use of personal data (LC 8899): This draft, restricting government employee use of individual's personal data off the site of government premises, may help to prevent a situation similar to the Department of Veterans Affairs breach.

Notice of security breach by government agencies (LC 8800): This draft would provide notice of a security breach of records held by government agencies, and require those agencies to meet standards for records retention and disposal. These are improvements over current law. However, in the context of expanding the existing Montana notice of breach law to government agencies, you may also wish to reexamine the definition of breach of security, found at section 30-14-1704(4)(a). That definition does not include all security breaches involving the compromise of specific personal information, such as name plus Social Security Number. Instead, the definition in existing law contains two limitations which will reduce notice. The definition is limited to: "unauthorized acquisition of computerized data that *materially* compromises the security, confidentiality, or integrity of personal information maintained by the agency, person or

business *and causes or is reasonably believed to cause loss or injury to a Montana resident.*" (emphasis added)

Under this definition, Montana law would not have required notice if the recent Department of Veterans Affairs breach had occurred at a Montana business, (or if LC 8800 were adopted, at a Montana government agency). The definition's requirement for "loss or injury" would allow the business or agency to say that because it wasn't known for many weeks who had the stolen laptop, there was no reason to know that there had been loss or injury and so the definition of security breach simply wasn't met.

The requirement in the definition of a security breach for loss or injury will excuse notice when notice should be given. For example, stolen information may be used months after a theft. A company or government agency could assert that there has not yet been loss or injury and so no notice of a security breach is required by the statute. There is frequently inadequate information about a security breach when it occurs to even determine who took information about Montana residents, much less whether it will be used to harm them. Many states, including Texas, Tennessee, Illinois, Nevada, New York and California, address this information gap by simply requiring notice in all cases where there is a security breach involving specific computerized, unencrypted personal data, without an additional trigger based on "risk of harm" or "loss or injury." As you consider extending Montana's existing requirement for notice of security breach to government entities, Consumers Union respectfully suggests that you also consider strengthening that requirement to eliminate "loss or injury" and "materially" in the definition of security breach.

Thank you for considering our comments on your important work.

Very truly yours,

Gail Hillebrand
Campaign Leader
Financial Privacy Now
Consumers Union