

Comments of U.S. PIRG:

Credit Report Freezes - Comment, Project No. P075420

Edmund Mierzwinski, U.S. PIRG Consumer Program Director

25 February 2008

### **Summary:**

U.S. PIRG believes that security freezes (or, to use the industry's preferred term "credit freezes") are the only effective means to prevent identity theft. Fraud alerts do not prevent the granting of credit; the industry's preferred and extremely profitable product, credit monitoring, of course, does not stop issuance of credit either. In fact, credit monitoring is only an after the fact warning.

Ideally, security freezes should be free to all consumers (not only past identity theft victims) and easy-to-use. If freezes were free, more consumers would use them. The reason that freezes are needed in the first place is that consumer reporting agencies and creditors do a poor job of protecting customer information, arguably in violation of both the Gramm-Leach-Bliley Act's Safeguards Rule and the Fair Credit Reporting Act's standards for data security. In any case, if freezes are not free, ideally a freeze should have only a one-time fee, then no fee to temporarily lift. You buy a lock for your house, you don't pay every time you unlock the door.

If freezes were easy-to-use, businesses and consumers would be happier with them. In states where businesses that issue credit have taken the time to think about the freeze, they've realized it should be simply, convenient and fast for a consumer to place or lift a freeze temporarily, and some state laws with 15-minute lifts reflect this. Simple and easy for consumers is simple and easy for business as well.

California passed its security freeze law in 2001. Starting in 2004, after we were successful in convincing Congress not to preempt state authority over identity theft protections, U.S. PIRG and Consumers Union<sup>1</sup> (later joined by AARP) launched a highly successful campaign to promote state identity theft protections, including the security freeze. To date, 38 more states and Washington, DC have enacted freezes.

So many states acted so quickly because the threat of identity theft is real. Now, even the credit bureaus have embraced the freeze. Of course, their version of the freeze is clunky, slow, burdensome and expensive. If all freezes were low-cost and easy-to-use and also were better promoted by the bureaus, we'd have more consumers using them.

If the FTC recommends a national security freeze law, it should recognize that in the 2003 FACT Act, one of the things that Congress got right was not to preempt further state action on identity theft. Any federal security freeze law or FTC rule should serve as a federal floor, not as a ceiling.

---

<sup>1</sup> See the U.S. PIRG/Consumers Union model law here:

<http://uspirg.org/financial-privacy-security/identity-theft-protection/model-law>

Finally, we believe that the costs of identity theft to the economy are staggering and that the benefits to society of improving consumer confidence in the safety of their financial information through the implementation of strong, free security freeze laws outweigh any costs to industry.

### **Discussion:**

Identity thieves have long exploited a major loophole in the credit-granting process. Credit grantors can often obtain credit reports as long as the application matches the report using two demographic items, name and Social Security number. A thief who obtains your Social Security number can apply for credit in your name at his or her address. It's really that simple. Social Security numbers can be harvested in a variety of ways without rocket-science or personal risk by thieves. Thus, identity theft has been a growth industry for over a dozen years.

Industry groups trumpet the limited federal responses to identity theft, such as fraudulent trade line blocking and fraud alerts, as comprehensive solutions. Most of these and other modest efforts are only available to assist victims in cleaning up identity theft. These tactics are not open to consumers seeking to prevent identity theft. Credit monitoring is largely beneficial to credit bureau bottom-lines, not consumers.

Led by California in 2001, and following a major campaign by U.S. PIRG and Consumers Union (later joined by AARP) 39 states and Washington, DC<sup>2</sup> have now enacted legislation designed to stymie identity thieves by closing the identity theft loophole that allows credit granting with inadequate verification of the applicant. Security freeze legislation solves the problem by giving consumers actual control over who can access their credit reports and when.

A freeze prevents new creditors from accessing your credit report. Ideally, the right to a freeze should be available to all consumers (although a few states have limited its availability to identity theft victims). The freeze closes the loophole that identity thieves have exploited, because most businesses will not issue new credit or loans to someone without first reviewing a credit report. Giving consumers control over access to their confidential information also better aligns data industry practices to the Fair Information Practices.<sup>3</sup>

When you want to obtain a loan, you can "lift" or temporarily "thaw" your credit report, by contacting the credit bureau.

Conversely, a so-called fraud alert is only available to consumers who believe that they are victims or active duty military personnel.<sup>4</sup> It doesn't actually stop the issuance of a credit report.

---

<sup>2</sup> See this Consumers Union page here for a list:

[http://www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html)

<sup>3</sup> The Fair Credit Reporting Act, more so than many other "privacy laws" is largely based on the FIPs, which impose openness, disclosure, secondary use, correction, and security principles on data collectors. But giving consumers greater control through the security freeze strengthens the relationship of the FCRA to both the security and usage principles. See "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy," Privacy Rights Clearinghouse, available at <http://www.privacyrights.org/ar/fairinfo.htm>

<sup>4</sup> Any consumer who believes that he or she may be a victim can obtain a "90-day" alert on all three repository files by contacting any of the three. A consumer who signs an "identity theft report" filed with a police agency, attesting

A creditor generally faces liability only if it fails to take reasonable verification steps before issuing credit based on a report containing a fraud alert.

### **History of the Security Freeze Concept**

In 1996, CALPIRG and U.S. PIRG published one of the earliest, if not the first, national reports on identity theft, "Theft of Identity: The Consumer X-Files." It included a detailed set of recommendations to stop identity theft before it starts, including a recommendation that "credit reports not be accessed without a consumer's permission."<sup>5</sup> Following discussions with experts, we and others then worked with California State Senator Herschel Rosenthal to introduce comprehensive identity theft legislation in 1997.

Although SB 930 did not pass, the process developed the concept of the security freeze: the consumer's right to freeze access to his or her credit report unless authorized through use of a PIN or other identifier. The actual term "security freeze" was not used in legislation until the following legislative session, 1999-2000, in a proposed bill, SB 1767, by State Senator Debra Bowen. Comprehensive security freeze legislation finally passed as SB 968 (Bowen) in 2001 and took effect on January 1, 2003.

Following passage of the 2003 Fair and Accurate Credit Transactions Act (FACTA) by Congress, the state PIRGs and Consumers Union, publishers of *Consumer Reports*, proposed a model state identity theft law<sup>6</sup> based on the areas that were not preempted by FACTA. The security freeze is the centerpiece of nine provisions, which can be enacted separately or as a package. Interest in passing the model law rapidly intensified in state legislatures<sup>7</sup>, following Choicepoint's February, 2005 notice to 163,000 consumers that it had sold their dossiers to identity thieves, followed by admissions of nearly 200 data breaches by other entities, affecting nearly 100 million Americans.

Since then, 39 more states and Washington, DC have enacted security freeze legislation, although not all laws have taken effect. The credit bureau lobby, through the Consumer Data Industry Association (CDIA), first stepped up its longtime opposition to strong bills in the states. It then launched a failed attempt in the Congress to enact a weak, preemptive federal security freeze law that would have only applied to previous identity theft victims.<sup>8</sup> That would have been like saying "You can't have a seatbelt until you've already been in a car crash."

---

that they are a victim, is eligible for a 7-year fraud alert. Active duty military personnel, especially those serving in Afghanistan or Iraq or other faraway posts, should take advantage of their fraud alert rights.

<sup>5</sup> Vermont requires oral consent before a report can be obtained for a credit purpose. Under federal law, any business with a "permissible purpose" can obtain a consumer report-- no consent is necessary. Of course, since an imposter could falsely provide consent, the security freeze with authorization is a stronger protection than a mere "consent" provision.

<sup>6</sup> See this Consumers Union page here for a list:

[http://www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html)

<sup>7</sup> The Choicepoint notifications were made nationally in response to a California breach notice law.

<sup>8</sup> See HR 4997, Financial Data Protection Act of 2006, as reported, 109<sup>th</sup> Congress, Reps. Steve LaTourette and Darlene Hooley.

Subsequently, last fall, in an effort to prevent remaining states from enacting even stronger security freeze laws, CDIA members announced that they would make expensive, clunky freezes available nationwide.

### **Key Security Freeze Issues**

**The freeze should be available to all consumers:** Giving only past victims the right to a freeze, as above, would have been like saying “You can’t have a seatbelt until you’ve already been in a car crash.”

**The freeze should be free or low-cost:** Consumers need to freeze all three national credit bureau reports to be effective. Expensive freeze laws will deter participation. Most states have enacted bills that are free to victims but most others impose varying fees on others. Yet, contrary to bureau claims, many states – including many with large populations --- have one-time or low fees. Here are a few examples: Indiana’s law is free to all consumers to freeze or lift. Several states, including Delaware, Nebraska and Washington, DC, have a “one-time” fee to freeze but no fee to lift. New Jersey and New York allow the first freeze for free and the consumer can lift the freeze temporarily for \$5. Montana caps all freezes or lifts at only \$3. In Colorado a freeze is free, but it could cost up to \$10 to lift or re-place the freeze. Several other states, including Massachusetts, have “\$5 to place and \$5 to lift” laws.

Some others have laws similar to the expensive bureau model: \$10 to place and \$10 to lift (again per bureau). Nevada has among the highest fees: \$15 to place a security freeze, \$18 to lift completely, and \$20 to lift for a single creditor. A few states unwisely only grant the freeze to previous victims.

**The freeze should be easy to use:** Industry has lobbied hard for clunky, 20th century freeze requests involving certified mail and 5-day turnarounds. PIRG argues that “Unless a credit freeze is user-friendly, it is useless because it won’t be used.” A number of states provide a 15-minute or “instant” lift and we understand that the industry no longer opposes this provision.

**The freeze should apply to all forms of credit, insurance and service applications:** Various industry lobbyists have attempted to narrow the definition of credit in the state and federal bills, which could limit the effect of the freeze. The definition of types of credit and other services covered by any freeze law should be as broad as possible,<sup>9</sup> including cell phones, insurance or other services, since thieves often go after these low-hanging fruit applications.

**No Preemption:** The PIRGs believe that the states should always remain as laboratories of innovation and will continue to oppose preemptive efforts on the security freeze and other identity theft protections. The credit bureaus rolled out their clunky national freeze to deter participation and to deter additional states from passing strong laws. They see the freeze as a

---

<sup>9</sup> All the state freeze proposals exempt pre-screening (use of credit reports to generate “pre-screened” lists for credit or insurance solicitation). Note, however, that the federal fraud alert right automatically opts a consumer out of pre-screening. Unfortunately, federal pre-screening rules preempt states from any stronger provisions on pre-screening, so the state freeze laws cannot take this obvious step.

threat to their relatively new billion dollar stream of income directly from consumers for “credit monitoring services,” priced at \$100/year or more. Credit monitoring doesn’t stop identity theft. Instead, consumers who want to sleep at night should have the government-guaranteed right to a low cost, easy-to-use security freeze. It’s the only way to stop identity theft before it starts.

**Promotion of the security freeze:** If more people knew about the freeze, more people would take advantage of it. We believe that the FTC needs to do a better job of making sure that the credit bureau websites and phone trees make the freeze option clear to consumers as an alternative to over-priced credit monitoring services offered by the bureaus. FTC should also determine whether any bureau omissions or commissions are actionable under the FCRA or the FTC Act.

The FTC should also look at advertising by the proliferation of relatively new third-party identity theft services offering, for example, products to automatically renew your 90-day fraud alerts and obtain your federal annual free credit reports. A security freeze may be a better option for many consumers than paying for these more expensive products, but consumers may be paying for these because they are heavily and possibly unfairly or deceptively advertised.