Testimony of

Consumer Federation of America
Consumers Union
Electronic Privacy Information Center (EPIC)
Privacy Consultant Mari Frank
Privacy Rights Clearinghouse
Privacy Times
U.S. Public Interest Research Group (U.S. PIRG)
World Privacy Forum

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

all intents and purposes, buy and sell comprehensive consumer information for decision-making about consumers, just as the regulated credit bureaus do. Although since its first reported[5] debacle Choicepoint has extended modest rights to consumers, these rights are not industry-wide and not guaranteed.

-- We also learned in the Choicepoint breach that the sloppy practices of financial companies extend well past losing unencrypted data tapes in shipping, failing to supervise third party processors or failing to prevent employee theft or computer hacking. Choicepoint actually sold detailed records on 145,000 consumers to identity thieves posing as customers.

-- We also learned that while the Gramm-Leach-Bliley Act imposed modest data security requirements (the so-called Safeguards rule[6]) on a wide range of financial and related firms holding customer data, that two major industry sectors were inexplicably left out of its definitions. Not only does the law fail to cover data brokers, it fails to cover third-party processors and servicers. Third party processors include companies such as Cardsystems, which is notorious for having had the largest reported breach, so far, which affected some 40 million credit and debit card numbers. Of course, the banks, credit card associations and other financial firms that contract with these processors should bear legal culpability for their failure to adequately supervise compliance with their own contractual requirements.

RECOMMENDATIONS:

In this testimony we make detailed recommendations for possible Congressional action. Although this committee has not yet drafted its own committee bill, we will comment on and compare key aspects of bills proposed in other committees. We urge the committee and the Congress, if you act, to adhere to the principles and recommendations below.

We say, “if you act,” because many of our organizations believe that the states are responding well and are concerned that if the Congress does act, it could do so in a way that permanently prevents further state privacy laws from being enacted. Such an outcome – despite a continuing wave of identity theft and fraud, occurring at the same time as firms continue to share and sell confidential consumer information in ways that were not even contemplated in 1999 when GLBA was enacted – would pose grave risks to consumer privacy and to ID theft prevention, and would neglect the strong lesson that good public policy leadership depends on both the states and the Congress.

A strong argument can be made that the states’ privacy leadership is adequate and continuing. Indeed, even before the 20 new states enacted breach notice laws of their own, other state Attorneys General forced Choicepoint and others to honor California’s notice requirements nationwide. In the detailed testimony below, we will provide numerous other examples of ways that the states have demonstrated privacy leadership and make the forceful argument that we have never had the so-called uniform credit system that the financial industry lobby claims, and that the nation has been the better for it.

Principles for Congress to respond to security breaches and other new privacy threats:

- Any new legislation should not preempt state authority to enact stronger privacy and identity theft laws. Let the states continue to lead and work together with the Congress to find solutions. A marketplace where a consumer can buy products from only one seller is not competitive, nor is a public policy marketplace of ideas which is restricted to Congress.
- We oppose the use of a so-called "harm trigger" in security breach notice proposals. Any data security breach notice legislation should not grant unnecessary and litigable discretion to the firms that lost data to make their own decision whether there is a "likely" or "reasonable" or even higher risk of misuse before notice is necessary. The best way to convince companies to keep data secure in the first place is to require notices whenever they do not. The fact that the company doesn't yet know whether or how the information will be misused should not be enough to excuse notice. Companies that lose information should not get to decide whether consumers need to take further action to protect their privacy. Consumers should be warned. As to the industry's so-called "sky is falling" argument that consumers might face too many notices, we are unaware that the California law has resulted in any frivolous notices. Below we also describe ways to make the notices clear.
- Any federal security freeze legislation should be available to all consumers, not only to past victims, as industry has insisted on in a few states. The intent of the security freeze is to protect all consumers, not only those with a strike against them already. Again, any federal law should allow states to continue to innovate and improve their laws. The newest security freeze law, in New Jersey, for example, builds on earlier efforts and contains many pro-consumer provisions not included in earlier laws.
- Congress should extend the requirements of GLBA's Safeguards rule to data brokers and third party processors.
- For data brokers, however, that is a necessary but not a sufficient condition. Data brokers should also be subject to a robust Fair Information Practices (FIPs)-based regulatory regime that, among others, gives consumers the rights to know about their file, to look at and correct their file, and control its use.
- Congress should fix the FACT Act. Too many of its identity theft remediation rights derive from bars that are too high for consumers to climb over or that provide only limited aid.
- Failure by firms to comply with any privacy rules should give victims a private right of action, as well as other Fair Information Practices based rights.

Finally, the issues before the Congress are fundamentally issues of privacy, as well as of identity theft prevention and data security. It is incumbent upon the Congress to understand that your response to these security breaches must recognize that these problems cannot be solved by merely imposing some additional security safeguard and notice requirements. Until the Congress recognizes that consumers need stronger privacy rights that extend to controlling the use of, as well as the misuse of what has aptly been called their financial DNA, these problems will continue to increase. Notice is not enough to protect privacy. Consumers need privacy rights.

Detailed Discussion

(1) The States Have Always Been Leaders On Privacy Protection

U.S. privacy law has always relied on state leadership; further, that state leadership has not stifled the economy in any way. Instead, the state leadership has stimulated eventual federal action and served to protect consumers better.

In 2004, two of our organizations, U.S. PIRG and Consumers Union, proposed a model state law[7] to enhance privacy and identity theft protection. It includes sections on the security freeze, security breach notification, insurance credit scoring regulation and other provisions.

- By the end of 2005, at least 20 states will have enacted security breach notification laws. At least nine of these laws have no harm trigger. (See Appendix 2 for a list of states. The list details which states have triggers.)
- Twelve states have enacted security freeze legislation. The most recent of these laws, New Jersey's, is the most innovative.

But these latest examples exist along a continuum of state privacy leadership often then emulated by Congress or regulators. Here are some other examples:

- As many as forty states had already enacted "do not call lists" before the FTC acted in 2003 to establish a national list.
- Seven states enacted free credit report on request laws before Congress enacted one in the 2003 FACT Act.
- California was first to enact a credit scoring disclosure law in 2000, after the FTC in the 1990s first supported the reform, then reversed itself and opposed score disclosure. Congress closely mirrored that provision in 2003 in the FACT Act.
- Two states – Washington and California – granted consumers the right to obtain business records from firms where identity thieves used their names before Congress added this benefit in the FACT Act.
- While California is most famous for taking advantage of the Sarbanes amendment to the Gramm-Leach-Bliley Act of 1999 to enact landmark affiliate sharing privacy rules in 2003,[8] several other states already had enacted opt-in regimes for financial data sharing and those laws have not been preempted.[9] In addition, North Dakota citizens, by referendum, overturned a bank-supported law that had eliminated their pro-privacy law requiring an opt-in before third party sharing.[10]
- Over a dozen states had enacted laws requiring the truncation of credit card numbers on consumer receipts before the provision was made nationwide in the FACT Act.
- While the FACT Act includes a modest provision requiring firms to provide a one-time notice that they may make negative reports to credit bureaus, Colorado has a much more privacy-friendly law requiring the credit bureaus themselves to provide annual notices to any consumers who have had negative information added to their reports.
- States have also led in other areas. California and Massachusetts enacted check float laws before the 1987 Expedited Funds Availability Act. California had enacted "Schumer box" type legislation before the enactment of the 1988 Fair Credit and Charge Card Act.

(2) Consequences of Misuse of Personal Information

The consequences of the misuse of confidential personal information – whether obtained through identity theft or a security breach-- are both economic and non-economic and begin but do not end with identity theft. It is important that any legislation recognize that "identity theft" is not the only negative outcome of security breaches.

Financial identity theft – where a consumer's social security number is used to assume their identity and open accounts in their name -- is a serious crime that has become more common in recent years as we have delved further into the "information age." Similarly, breaches involving acquisition of credit or debit card numbers can result in massive consumer fraud. The problem can be especially difficult when a debit card theft results in a thief draining a consumer's checking account.[11]

According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions about $48 billion annually and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and may spend hundreds of hours to clear their credit reports. A new study by the Identity Theft Resource Center provides comprehensive details on the types of fraud that occur and on the amount of out-of-pocket expenses and time victims spend clearing their names.[12] The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

Security breaches can certainly lead to financial identity theft but also result in other crimes. Increasingly, according to the Privacy Rights Clearinghouse and the Identity Theft Resource Center, consumers are becoming victims of criminal identity theft, where their confidential information is used to assume their identity for criminal purposes.

Confidential consumer information can also be misused for stalking and for tracking down victims of domestic violence who've attempted to hide from their abusers. Data on a consumer's financial or medical history can also be used to publicly embarrass him or her.

Information stolen may be used to commit terrorism. As is well-documented, the 9/11 terrorists used ID theft to get credit cards, apartments, and rental cars. In at least one case, one male hijacker successfully used the Social Security Number of a long-dead New Jersey woman.

(3) Data Brokers Evade The Fair Credit Reporting Act. A Robust Regulatory Regime Is Needed

In 2005, breaches have occurred in banks and their affiliates, retailers, card processors, government agencies and universities. Yet, there are a number of factors that set the breaches occurring at Choicepoint and Lexis-Nexis, the two data brokers with reported breaches, apart. First, the firms are virtually unregulated.

The 1970 Fair Credit Reporting Act (FCRA) was the nation's first major privacy law. Despite its flaws, which make identity theft too easy and also enable mistakes in credit reports that lead to consumers paying too much for credit or even being denied credit, the FCRA is a robust law that gives consumers Fair Information Practices[13] based rights. For example, consumers have the

right to know about, inspect, dispute and correct their files. The FCRA requires purpose specificity before a report can be accessed.

Yet the data brokers, including Choicepoint and Lexis-Nexis, have designed their business models to evade the Fair Credit Reporting Act's protections. In a December 2004 complaint[14] to the FTC, EPIC points out that:

> Americans face a return to the pre-FCRA era if companies like ChoicePoint can amass dossiers on Americans without compliance with any regime of Fair Information Practices. That era was marked by unaccountable data companies that reported inaccurate, falsified, and irrelevant information on Americans, sometimes deliberately to drive up the prices of insurance or credit. …ChoicePoint sells a number of FCRA products in the employment screening, tenant screening, and criminal background check fields. But the company also sells two products, "AutoTrackXP" and "Customer Identification Programs" outside of the FCRA's protections. AutoTrackXP is a database of 17 billion records that includes Social Security Number, addresses, property and vehicle information, and other information (citations omitted).

In a separate proposal, EPIC's Chris Hoofnagle and law professor Daniel Solove explain how data brokers exploit flaws in several poorly written definitions in the FCRA:

> The FCRA applies to "any consumer reporting agency" that furnishes a "consumer report." The definition of "consumer reporting agency" is any person who "regularly engages" in collecting information about consumers "for the purpose of furnishing consumer reports to third parties." This definition turns on the meaning of "consumer report," which is the key term that defines the scope of the Act. Unfortunately, the FCRA has a poorly drafted definition of "consumer report" that has allowed some to unduly narrow the Act's coverage. The Act conditions the definition of "consumer report" on how the information is used. That is, a "consumer report" is any communication bearing on a consumer's character or general reputation *which is used for* credit evaluation, employment screening, insurance underwriting, or licensing. Although the FCRA was passed to limit the uses of personal information in evaluating people, a literal reading of its definition of "consumer report" makes the law inapplicable if information is used for an unauthorized purpose beyond those enumerated in the Act. One could argue, for instance, that a criminal using credit information for fraud has not triggered the FCRA because fraud is not an authorized use. These problems in the definition of "consumer report" have allowed data brokers to avoid being regulated by the FCRA.[15]

In 1997, the data brokers convinced the Federal Trade Commission to approve their proposed self-regulatory scheme, under the so-called Individual References Services Group (IRSG) Principles. The Lexis-Nexis Privacy Policy states that "The IRSG consulted with the FTC in formulating its principles and auditing measures, and the FTC approved these principles and audit measures.[16]" In its "Individual Reference Services: A Report to Congress," the FTC in October 1997 stated the following: "The Commission commends members of the IRSG Group for the commitment and concern they have shown in drafting and agreeing to comply with an innovative and far-reaching self-regulatory program.[17]"

While the IRSG is now apparently defunct, the data broker business grew and flourished under this lax FTC oversight. Again, according to Hoofnagle and Solove:

> In the absence of statutory regulation, data brokers have adopted self-regulatory rules known as the Individual Reference Services Group (IRSG) Principles. The Principles set forth a weak framework of protections, allowing companies to sell non-public personal information "without restriction" to "qualified subscribers," which includes law enforcement agencies. "Qualified subscribers" need only state a valid purpose for obtaining the information and agree to limit re-dissemination of information. Under IRSG, individuals can only opt-out of the sale of personal information to the "general public," but ChoicePoint does not consider its customers to be members of the general public. The IRSG Principles were carefully crafted in order to ensure maximum flexibility by commercial data brokers. They have failed to set forth a reasonable degree of protection for individuals, and in fact, it was while data brokers were operating under these principles that the major privacy breaches occurred.[18]

Further, it is useful to examine the scope of the data broker enterprises and question whether it is good public policy to leave them unregulated, when you consider their power over both the government and private sectors. Choicepoint, for example, is the largest information broker in the United States. The company has amassed more than 19 billion records and has acquired a large number of smaller companies that obtain everything from criminal history records and insurance claims to DNA databases. The private sector and increasingly government rely on the data provided by Choicepoint to determine whether Americans get home loans, are hired for jobs, obtain insurance, pass background checks, and qualify for government contracts.

Not only does Choicepoint operate without regulatory scrutiny, employment or credit or insurance decisions are often made based on mistakes in their database, as numerous stories and studies have pointed out. According to a recent report[19] by Privacy Activism based on a review of a small number of reports held by Choicepoint and a second data broker, Acxiom, "The majority of participants found errors in even the most basic biographical information: name, social security number, address and phone number (in 67% of Acxiom reports, 73% of ChoicePoint reports). Moreover, over 40% of participants did not receive their reports from Acxiom -- and the ones who did had to wait an average of three months from the time they requested their information until they received it." While the study from Privacy Activism is only a pilot based on a small sample, it suggests that there may be serious problems with data broker data.

The data brokers have unfortunately resurrected the Bart Simpson defense ("it's not my fault") used by the credit bureaus in the early 1990s to delay needed remedial legislation to improve their accuracy rates. In the 1990s, credit bureaus claimed that they merely reported what the creditors furnishing information to them provided. The data brokers claim that they simply report public record information and that any errors aren't their fault.

But what if they mix up two accurate public records and report them on the wrong consumer? Shouldn't data brokers have duties to ensure that their data are accurate, just as credit bureaus do? Doesn't it make sense to impose a FCRA-like regulatory structure on their business model?

The companies' reliance on public records brings up another matter—the purpose of and availability of public records in the first place. The firms often claim that they have some sort of a "right" to aggregate and re-sell public records for whatever purpose that they want. After all, the records are public, they say. But originally, the records weren't aggregated for new uses by private third parties. They were simply used, for example, to determine if the government was assessing your house accurately, compared to how it assessed your neighbor's. Hoofnagle and Solove point out, "Public records are essential for effective oversight of government activities, but commercial data brokers have perverted this principled purpose, and now public records have become a tool of businesses and the government to watch individuals."

If the government is going to allow use of public records for all these secondary purposes, then it should grant public record subjects greater rights when the records are aggregated and sold for these secondary purposes by data brokers.

(4) Approaches to Fair Information Practices-based Regulation of Data Brokers.

We believe that S. 500 (Bill Nelson) and S. 768 (Schumer-Bill Nelson) offer reasonable Fair Information Practices-based approaches to regulating data brokers through FTC rulemaking. But it is critical that the Congress not delegate all authority to the FTC, which failed to regulate the brokers in 1997. Security breaches and the effects on consumers of the ongoing maintenance of files on most Americans by information brokers are issues too important to be delegated in full to any regulatory agency.

Hoofnagle and Solove, in their "Model Privacy Regime" describe the framework which any new law should be based on. In our view, data brokers are most like consumer reporting agencies (credit bureaus) and should be regulated by a strict FCRA-like privacy regime, rather than merely subjected to the very general Safeguards rule of the Gramm-Leach-Bliley Act.

Any federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness.

(5) We support a strong security breach notification law without any so-called harm trigger.

Our organizations believe that any federal notice-of-breach law should do the following:

• Cover paper and computerized data.
• Cover government and privately-held information.
• Should not except encrypted data, due to weaknesses in encryption technologies. Consumers need to know every time an unauthorized person has accessed his or her personal identifying information, such as last name, address or phone number plus a social security number, driver's license number, or account number, particularly if robust encryption is lacking or compromised. This information is enough to open new credit accounts.
• Should not except regulated entities, such as financial institutions covered by the bank regulator guidelines.[20]
• Should have no loopholes, sometimes called "safe harbors."

• Should be triggered by the acquisition of information by an unauthorized person. There should be no additional trigger such as a judgment by the breached entity that there is a "reasonable risk of identity theft."
• Should require that any law enforcement waiting period must be requested in writing and be based on a serious impediment to the investigation.
• Should give consumers who receive a notice of breach access to the federal right to place an extended fraud alert (which would otherwise require filing a police report alleging fraud or identity theft) and should provide for free credit reports and/or credit monitoring for an adequate period of time, with no automatic conversion of the "free" service to a paid service.[21]

A number of breach notification bills have been proposed in other committees. The bills differ primarily in the entities to be covered, the numbers and types of safe harbors, the scope of preemption of better state laws and whether there is a harm trigger before consumers must be notified. Our organizations strongly believe that consumers should get notice of each breach which reaches, or is reasonably believed to have reached, the consumer's personal identifying information, such as social security number, account number, drivers' license number, credit card or debit card number, and similar information.

- Notice will not be required if a hacking or lost data incident does not include specific personal information.
- In all other cases, notice should be required, with no special exceptions for particular industries.
- The company that had the security breach should not be allowed to decide whether or not to give the notice.

Entities that hold our data say that consumers shouldn't be flooded with notices. They propose that notice of a security breach should be required only if there is a risk of harm to consumers. This argument fails to consider the following:

- Any standard that hinges on a determination of likely risk of harm means that consumers get no notice when no one knows who took the data, or why.
- Information can be taken from a data broker, retailer, or bank and used with a different entity to open a new credit account. The business whose security was breached has no way to know how the information is, or might be, used with someone else and may therefore claim there is no risk. For example, after the loss of a back up tape reported to contain more than three million unencrypted names and social security numbers, CitiFinancial still claimed that "there is little risk" to consumers.
- A harm trigger leaves the burden of uncertainty on the consumer: Any trigger that requires a risk of harm may leave consumers in the dark when the breached company doesn't know who intruded into their data system, or why the intruder acted. A company might argue that it can't conclude or know that there is a risk of harm if it doesn't know the identity or purpose of the intruder. If the company doesn't know who breached the system or stole the laptop or the back-up tape, it can claim that it doesn't know whether or not consumers are at risk. Any standard that ties notice to knowledge of a risk of harm leaves consumers with no notice in the event of incomplete facts about the data security breach.

- A harm trigger that the breached entity applies lets the company with an interest in keeping the data breach secret be the one who decides if notice is required. This is an inherent conflict of interest.
- When businesses know that they must tell consumers about every security breach that reaches certain personal information, they may choose to invest more in data security, preventing more breaches. Thus, a strong notice law can protect consumers partly by encouraging better security, which reduces the number of breaches and thus the number of notices.
- Consumers need to know *every* time an unauthorized person has accessed his or her personal identifying information, such as last name, address or phone number plus a social security number, driver's license number, or account number. This information is enough to open new credit accounts.

Information can be taken from a data broker, retailer, or bank and used with a different entity to open a new credit account. The entity who had the security breach has no way to know if the stolen information is, or might be, used with someone else.

Further, according to studies by the FTC, the Identity Theft Resource Center and the Privacy Rights Clearinghouse, consumers, in many cases, do not know how they became victims of identity theft. According to the FTC report released in 2003, "about half" of victims knew how the thief obtained their personal information.[22] So, about half of victims do not know, and could benefit from security breach notices, especially since many victims do not discover that they are victims for months after the crime.

Victims of breaches have no idea if or when their personal info will be used to commit ID theft. There is also some evidence that some thieves are putting the data on the shelf so to speak, until the heat is off, and then using the Social Security Number, Date of Birth or other information to apply for new credit at a later date, well after the limited initial 90-day fraud alert has been removed.

As to the argument that the notices will get lost, Evan Hendricks of the *Privacy Times* has proposed a unique solution. He proposes that any federal security breach notice legislation establish a federal seal that must appear below the return address on notice envelopes and could not be used for any other purpose. He further proposes that the seal be a privacy form of the poison control authority's "Mr. Yuck" and that its misuse for other non-breach notification purposes be considered a crime.

(6) Principles for Strong Security Freeze Legislation

Identity theft relies on two things: easy availability of your Social Security Number (financial DNA) and a loophole in the credit granting process. First, your Social Security Number is both ubiquitous and easy to obtain. If Congress wants to protect privacy, it must put the Social Security Number back in the bottle (see below). Second, identity thieves don't need to obtain your credit report, which is actually difficult for an impostor to obtain (without inside access). So, the identity thieves simply obtain your Social Security Number, then they ask a creditor to obtain your credit report and to then issue credit in your name to them, pretending to be you.

Identity theft is epidemic because it relies on these two simple factors—get a fraudulent SSN and apply for credit.

Requiring consumer consent before issuing the report would be a useful Fair Information Practice (it isn't required for credit purposes except in Vermont) but that wouldn't work to prevent identity theft, because thieves would simply grant false or fraudulent consent.

The solution, then, is to short-circuit the quick access to credit, which relies on the creditor obtaining your credit report and/or credit score. The security freeze prevents access to your credit report to new creditors, thereby closing the loophole that the thieves exploit.

We call this a "security freeze," which allows consumers to block access to their credit reports, and the credit scores derived from those reports, until they affirmatively unfreeze the consumer credit files. Most businesses will not issue new credit or loans to people without first reviewing their credit report or credit score. If the credit file is frozen and an imposter applies for credit in the name of a consumer, a creditor would be very likely to deny the imposter's application, because the security freeze would prevent the prospective creditor from checking the consumer credit report or score. This protects both the consumer and the business from being harmed by identity theft. Thus, giving Americans the right to place a security freeze on their credit files helps prevent identity thieves from achieving their ultimate goal – opening up new credit accounts to accumulate debt in the consumer's name.

Some of the very first security freeze laws were heavily influenced by the credit bureaus and the financial industry lobby, which claimed that they needed all sorts of time to freeze or unfreeze accounts and that consumers should pay a hefty price. Industry also argued that the right to freeze should be limited to previous identity theft victims. That makes no sense. The purpose of the freeze is to give any consumers who are not in the market for credit the right to prevent thieves who apply for credit in their names from completing their fraudulent applications. Instead, they are frozen out in the cold. Industry also successfully inserted an exception in most state laws for pre-screening of credit and insurance solicitations. Even the FACT Act states that consumers who request a fraud alert automatically are "opted-out" from pre-screening, which has been a vector for identity theft.

Of course, the freeze should have reasonable exceptions. For example, existing creditors should have the right to access your report. But the freeze should clearly block new applications for credit and the issuance of credit scores to any new creditor.

New Jersey's security freeze law is among the newest and includes several important innovations. While the early freeze laws reluctantly accepted the industry claim that 5 days was necessary to freeze or unfreeze a report, the New Jersey law requires a rulemaking process to eventually obtain a 15 minute unfreeze. Just as we have "instant credit," we should have "instant freeze."

If a security freeze is too expensive or is inconvenient, consumers won't use it. Among the other improvements of the New Jersey law are the following: (1) the credit reporting agencies must provide a convenient method of use, such as phone or internet; (2) the credit reporting agencies must lift the freeze as quickly as possible, with the goal being within 15 minutes; (3) the freeze is free to put on and $5 to temporarily lift; and (4) it is available to all consumers. Other states'

freezes authorize but don't require a convenient method of use; allow up to three days to lift; cost more; and, in a few states, are limited to Identity Theft victims only.

Any federal security freeze law should apply to all new applications, not merely applications defined as narrow "credit" purposes under the FCRA. Identity thieves, according to the FTC, open all sorts of accounts they could be frozen out of: credit cards, loans, telephone service, internet accounts, insurance, and others. Also, identity thieves sometimes rent housing in victims' names, a transaction that is not new account fraud, strictly speaking, but does involve a credit report check.

(7) Protecting SSNs

Numerous businesses and organizations demand that a person provide a Social Security Number and then use that number as a password for access to accounts and data. Many schools, the military and other organizations use Social Security Numbers on identification cards, thus ensuring that when a wallet is lost or stolen, one's Social Security Number is exposed. The use of Social Security Numbers is so extensive that as simple a transaction as signing up for cell phone service often requires disclosing one's Social Security Number.

This makes it easy for identity thieves. It is well-documented, for example, that identity thieves will often seek employment as temporary office employees, solely to harvest SSN and other bits of "financial DNA."

Social Security numbers (SSNs) were never meant to become a de facto national identifier, but that's exactly what has happened. A consumer's nine-digit Social Security number could be on file in the databases of their bank, insurance company, local department store, doctor's office, various government agencies, schools, and countless other businesses. If that's not bad enough, Social Security numbers can be bought for as little as $35 on internet web sites that sell personal data culled from public records.

In this information age, SSNs have become widely accessible and often serve as the master key used by crooks to steal identities and unlock credit files. Congress should restrict the sale, collection, use, sharing, posting, display and secondary use of Social Security numbers (SSNs). Such restrictions should include:

- Ban the collection and use of SSNs by private entities or by government except when necessary to a transaction and there is no alternative identifier which will suffice. Prohibit firms from "coercing" consumers into providing SSNs as a condition of doing business with them.
- Ban the sale, posting, or display of SSNs. There is no legitimate reason to post or display individuals' Social Security numbers to the public.
- Ban the printing or encoding of SSNs on government and private checks, statements, and the like.
- Ban the use of the SSN for government or private identifiers, except for Social Security purposes. This includes banning the use of the SSN, or a variation or part of it, for government and private programs such as Medicare, health insurance, driver's licenses or driver's records, and military, student, or employee identification. Any provision banning

the printing of SSNs on identifying cards should also prohibit encoding the same information on the card.

- Any legislation should look harshly on requests from credit bureaus and others demanding "routine exceptions" for their uses. Unless credit bureaus and others are weaned from their over-reliance on the Social Security Number as a unique identifier, we will not succeed in protecting the SSN from misuse.

(8) Fixing the FACT Act

A consumer should be able to access more of his or her Fair and Accurate Credit Transactions Act (FACT Act) rights, such as the extended fraud alert, before becoming an ID theft victim. Further, one of the key FACT Act rights is tied to a police report, which victims still report difficulty in getting and using.

The FACT Act has made some things more difficult for identity theft victims, according to information provided to Consumers Union by nonprofits and professionals who assist identity theft victims.

Moreover, the FACT Act gives only limited rights to those who have not yet become victims of identity theft, and the FACT Act fails to offer a pure prevention tool for all consumers (only the freeze is a pure prevention tool). A consumer who asserts in good faith that he or she is about to become a victim of identity theft gets one right under the FACT Act—the right to place, or renew, a 90 day fraud alert. However, this type of alert places lower obligations on the potential creditor than the extended alert, which is restricted only to identity theft victims.

Here are some key ways to make the FACT Act work for victims:

• Its initial fraud alert should be one year, not 90 days.
• Its extended alert and other victims' rights, other than blocking of information, should be available to all identity theft victims who fill out the FTC ID theft affidavit under penalty of perjury.
Business records should be available to any consumer who fills out the FTC ID theft affidavit under penalty of perjury (the consumer should not additionally be required to file a police report).
• Consumers who receive a notice of security breach should be entitled to place an extended fraud alert.
• Consumers who place a fraud alert have the right under the FACT Act to ask for a free credit report, but this should be made automatic.

Also, under the FACT Act, the FTC and the federal financial institution regulators are charged with developing a set of red flag "guidelines" to "identify possible risks" to customers or to the financial institution. However, the FACT Act stops with the identification of risks. It does not require that financial institutions do anything to address those risks once identified through the not-yet-released guidelines. The presence of a factor identified in the guidelines does not trigger a statutory obligation to take more care in determining the true identity of the applicant before granting credit. Congress should impose a plain, enforceable obligation for creditors to contact

the consumer to verify that he or she has in fact sought credit when certain indicators of potential identity theft are present.

There is also work to do outside of the FACT Act, including work to develop a police report that could be given to victims that is sufficiently similar, if not uniform, across jurisdictions, so that the victim does not find creditors or businesses in another jurisdiction refusing to accept a police report from the victim's home jurisdiction.

We would like to make other changes to the FACT Act, such as providing consumers with a private right of action in more circumstances to improve its enforcement. The proposals above, however, represent minimal, consensus ideas that should be agreeable to all parties.

Conclusion

This year, the "year of the breach notice," has highlighted needed changes to federal privacy laws to protect consumers. It has also highlighted the longstanding leadership of states in responding to privacy threats. Federal law should always serve as a floor, not a ceiling. If Congress does a good enough job, industry has no worry at all of so-called "balkanization." If, however, Congress does a less adequate job, then states can respond quickly to new privacy problems. Otherwise, we would likely have to wait for yet another scandal to convince Congress to act again.[23]

Recall that even Enron wasn't a large enough scandal to move the Congress to enact corporate reform, it also took Worldcom. We can only hope that the numerous security breaches in 2005, including two identified at virtually unregulated data brokers, equals enough of a "privacy Enron" or a "privacy Valdez" to convince the Congress to enact non-preemptive, privacy rights legislation. We look forward to working with the committee to do so.

After Endnotes:

Appendix 1: List of Security Breaches from Privacy Rights Clearinghouse
Appendix 2: List of States with Security Breach Laws and Whether Their Laws Have Harm Triggers (Consumers Union)
Appendix 3: List of States with Security Freeze Laws (U.S. PIRG)

[1] Consumer Federation of America (www.consumerfed.org), Consumers Union (www.consumer.org), Electronic Privacy Information Center (www.epic.org), Privacy Consultant Mari Frank (www.identitytheft.org), Privacy Rights

Clearinghouse (www.privacyrights.org), Privacy Times (www.privacytimes.com) and World Privacy Forum (www.worldprivacyforum.org).

[2] Disclosure of Nonpublic Personal Information, Public Law 106-102, 15 U.S.C. § 801-6809, see Section 6807, Relation to State Laws, available at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6807 last visited 19 September 2005. "(b) Greater protection under State law. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter…"

[3] PL 108-159, 12/04/03.

[4] 15 USC § 1681 et seq.

[5] Numerous news stories have described Choicepoint's legal efforts to settle at least one previous undisclosed breach. See, e.g., "ChoicePoint suffered previous breach," Associated Press, 2 March 2005, available at http://www.msnbc.msn.com/id/7065902/ last visited 19 September 2005, which reports on a 2002 episode: "A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud, Assistant U.S. Attorney Mark Krause in Los Angeles said Wednesday."

[6] Disclosure of Nonpublic Personal Information, Public Law 106-102, Title V, Subtitle A, 15 U.S.C. § 801-6809 (Financial Privacy) Section 501(b) of the law required the FTC to develop its Safeguards Rule.

[7] See http://www.pirg.org/consumer/credit/model.htm or http://www.consumersunion.org/pub/core_financial_services/001732.html (both last visited 19 September 2005).

[8] Although SB 1 (Speier) was upheld by the U.S. District Court, the Ninth Circuit recently over-ruled parts of it and remanded others back to the lower court. EPIC maintains a page http://www.epic.org/privacy/preemption/abavlockyer.html (last visited 19 September 2005) describing the issues before the court and a link to the Ninth Circuit decision remanding the case. http://www.epic.org/privacy/preemption/abavlockyerninecir.pdf (last visited 19 September 05).

[9] See, e.g, letter of 25 August 2004 finding no preemption from the FTC to Illinois Commisioner of Banks and Real Estate D. Lorenzo Padrone at http://www.ftc.gov/os/2004/09/040903letterglbpadron.pdf last visited 21 September 2005

[10] See testimony of the Honorable James Kasper, North Dakota House of Representatives, before this committee on 19 September 2002, available at http://banking.senate.gov/02_09hrg/091902/kasper.htm last visited on 20 September 2005.

[11] Credit cards are regulated under the Truth In Lending Act, which has a statutory $50 consumer liability limit for fraud. Debit cards (ATM cards which can be used with or without a secret PIN) are regulated under the weaker Electronic Funds Transfer Act, which provides for three tiers of consumer liability ranging from $50 to $500 to all of the money in a consumer's account and any linked overdraft or checking accounts, depending on when a consumer gives notice of the fraud. While most institutions have prominently but voluntarily limited debit card liability to $50 in some circumstances, this protection is subject to numerous exceptions. Further, with a debit card fraud, until the bank completes a reinvestigation and permanently reinstates the account, even the consumer who is eventually made whole may face additional problems due to the temporary loss of funds. Ideally, since debit cards can be used without PIN numbers, the fraud limits of the EFTA should be amended to be equivalent to those of the Truth In Lending Act (harmonized upward). The additional TILA protections (Fair Credit Billing and other dispute rights) should also be extended to debit cards.

[12] See "Identity Theft: The Aftermath 2004," September 2005, by the Identity Theft Resource Center, available at http://www.idtheftcenter.org/aftermath2004.pdf last visited 21 September 2005. The study updates a similar 2004 report by the center and also the original report in the series, "Nowhere To Turn: Identity Theft Victims Speak Out," by CALPIRG and the Privacy Rights Clearinghouse, 1 May 2000, available at http://calpirg.org/CA.asp?id2=3683&id3=CA& last visited 21 September 2005.

[13] The Fair Information Practices (FIPs) require collection limitation, purpose specificity, disclosure to and correction rights for data subjects, data security and limits on secondary use without consent. The FIPs were originally proposed by a 1973 task force of the Health, Education and Welfare Department. The HEW task force recommendations were embodied in the 1974 U.S. Privacy Act (applying to government uses of information) and in the 1980 "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" of the international Organization of Economic Cooperation and Development (OECD) and have been incorporated into the European Union Data Directive and other European privacy laws. The FCRA, the Video Privacy Protection Act and a few other U.S. laws applying to the privacy sector incorporate aspects of the FIPs. A comprehensive history is

maintained by the Privacy Rights Clearinghouse at http://www.privacyrights.org/ar/fairinfo.htm last visited 21 September 2005.

[14] See http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html last visited 19 September 2005

[15] Solove, Daniel J. and Hoofnagle, Chris Jay, "A Model Regime of Privacy Protection (Version 2.0)" (April 5, 2005). GWU Law School Public Law Research Paper No. 132; GWU Legal Studies Research Paper No. 132. http://ssrn.com/abstract=699701 last visited 21 September 2005.

[16] See Lexis-Nexis Data Privacy Policy, http://www.lexisnexis.com/clients/iip/dataPrivacy.htm last visited 18 September 2005.

[17] See Individual Reference Services, A Report to Congress, Federal Trade Commission, December 1997, http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm last visited 19 September 2005.

[18] Hoofnagle and Solove, *op. cit.*

[19] See "Data Aggregators: A Study of Data Quality and Responsiveness," Privacy Activism, May 2005, http://www.privacyactivism.org/Item/220 last visited 19 September 05.

[20] The bank regulator "guidelines" may not have the full force of law, except where agencies have codified them as final rules. We also note positively that, despite requests for preemption, the guidelines do not preempt stronger state laws. See discussion at page 10 of "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 9 March 2005, available at http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf last visited on 21 September 2005.

[21] See "Marketer of "Free Credit Reports" Settles FTC Charges,"16 August 2005. The FTC fined Experian $950,000 and ordered it to pay refunds to consumers for deceptive advertising of its subscription-based credit monitoring services as free, both on its website freecreditreport.com and through an attempted association with the government-mandated free credit report website annualcreditreport.com. See http://www.ftc.gov/opa/2005/08/consumerinfo.htm last visited 19 September 2005.

[22] See page 30, Federal Trade Commission Identity Theft Survey Report," prepared by Synovate Corporation, September 2003, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf last visited 21 September 2005.

[23] See "Preemption Of State Consumer Laws: Federal Interference Is A Market Failure," by U.S. PIRG's Ed Mierzwinski, which appeared in the Spring 2004 (Vol. 6, No. 1, pgs. 6-12) issue of the Government, Law and Policy Journal of the New York State Bar Association. The article includes a major section on the history of the FACT Act It is available here http://www.pirg.org/consumer/pdfs/mierzwinskiarticlefinalnysba.pdf last visited 21 September 2005. Also see generally, PIRG's "Financial Preemption" http://www.stopatmfees.com/occpirg.htm and "Stronger State Laws" pages at http://uspirg.org/uspirg.asp?id2=17742&id3=USPIRG& for information about growing threats to stronger state privacy, financial, public health and environmental laws. Both last visited 21 September 2005.

Appendix 1: Summary of Data Breaches Reported In 2005

Compiled by Privacy Rights Clearinghouse www.privacyrights.org

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	ID thieves accessed	145,000
Feb. 25 , 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	Hacking	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer	8,900
March 20, 2005	Northwestern Univ.	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas	Hacking	5,000
March 22, 2005	Calif. State Univ., Chico	Hacking	59,000
March 23, 2005	Univ. of CA, San Francisco	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	unknown
April ?, 2005	Georgia DMV	Dishonest insider	"hundreds of thousands"
April 5, 2005	MCI	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group	Stolen computer	185,000
April 11, 2005	Tufts University	Hacking	106,000
April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC	Hacking	180,000
April 14, 2005	Calif. Fastrack	Dishonest Insider	4,500
April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 18, 2005	DSW/ Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
April 26, 2005	Mich. State Univ's Wharton Center	Hacking	40,000
April 26, 2005	Christus St. Joseph's Hospital	Stolen computer	19,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000

April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
May 2, 2005	Time Warner	Lost backup tapes	600,000
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 5, 2005	Purdue Univ.	Hacking	11,360
May 7, 2005	Dept. of Justice	Stolen laptop	80,000
May 11, 2005	Stanford Univ.	Hacking	9,900
May 12, 2005	Hinsdale Central High School	Hacking	2,400
May 16, 2005	Westborough Bank	Dishonest insider	750
May 18, 2005	Jackson Comm. College, Michigan	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 19, 2005	Valdosta State Univ., GA	Hacking	40,000
May 20, 2005	Purdue Univ.	Hacking	11,000
May 26, 2005	Duke Univ.	Hacking	5,500
May 27, 2005	Cleveland State Univ.	Stolen laptop	44,420
May 28, 2005	Merlin Data Services	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 29, 2005	Bank of America	Stolen laptop	18,000
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
July 6, 2005	City National Bank	Lost backup tapes	unknown
July 7, 2005	Mich. State Univ.	Hacking	27,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000
Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000

Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Sept. 10, 2005	Kent State Univ.	Stolen Computers	100,000
Sept. 15, 2005	Miami Univ.	Exposed Online	21,762
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000)	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
TOTAL			**50,721,749**

Consumers Union

Notice of Security Breach State Laws

Last updated August 31, 2005

Arkansas – SB 1167, Passed into law in 2005. Law provides notice to consumers of breach in the security of unencrypted computerized, personal information which is held by a person or business. Notice is not required if no reasonable likelihood of harm to consumers.

California - Civil Code Sec. 1798.80-1798.82, effective July 1, 2003. Requires notice to consumers of breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or a government agency.

Connecticut – SB 650, Passed into law 2005, effective January 1, 2006. Requires notice of security breach by persons who conduct business in the state and have a breach of the security of unencrypted computerized data, electronic media or electronic files, containing personal information. Notice is not required if the breached entity determines in consultation with federal, state, and local law enforcement agencies that the breach will not likely result in harm to the individuals.

Delaware – HB 116, signed June 28, 2005. Requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons doing business in the state. Covers sensitive personal information including medical information. Violations trigger triple damages plus attorneys fees.

Florida – HB 481, signed June 14, 2005, Chapter 2005-229. Effective July 1, 2005. Requires notice to consumers of material breach in the security, confidentiality or integrity of computerized, unencrypted personal information held by a person who conducts business in the state. Time limits for the notice to be given and penalties if notice is not given on time. Penalties do not apply to government agencies.

Georgia – SB 230, Passed into law in 2005, effective May 6, 2005. Requires notice of breach that compromises the security, confidentiality, or integrity of computerized personal information held by a data broker.

Illinois – HB 1633, Public Act 094-0036, signed June 16, 2005, effective Jan. 1, 2006. Requires notice to consumers of breach in the security, confidentiality, or integrity of personal information in system data held by a person or a government agency.

Indiana – Act No. 503, Passed into law in 2005, effective June 30, 2006. Law provides notice to consumers of breach in the security, confidentiality, or integrity of computerized personal information held by a government agency.

Louisiana – SB 205, Act 499, signed July 12, 2005, effective January 1, 2006, or such later time if the Attorney General completes regulations. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. No notice if, after a reasonable investigation, the data holder determines that there is "no reasonable likelihood" of harm to customers. Further exemption for those financial institutions which are in

compliance with federal guidance. Authorizes civil actions to recover actual damages.

Maine – LD 1671, signed June 10, 2006, effective January 31, 2006. Covers only information brokers. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information to residents of the state. Provides civil penalties for violations.

Minnesota – H.F. 2121, Passed into law 2005, effective January 1, 2006. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Does not apply to financial institutions or HIPAA entities.

Montana – HB 732, Passed into law in 2005, effective March 1, 2006. Law provides notice to consumers of breach in security, confidentiality, or integrity of computerized personal information held by a person or business if the breach causes or is reasonably believed to have caused loss or injury to a Montana resident.

Nevada – SB 347, Passed into law 2005, effective January 1, 2006. Requires notice of breach of the security, confidentiality, or integrity of unencrypted computerized personal information by data collectors, which are defined to include government, business entities and associations who handle, collect, disseminate or otherwise deal with nonpublic personal information.

North Dakota – SB 2251, Passed into law in 2005, North Dakota Century Code Chapter 51-30, effective June 1, 2005. Requires notice of a breach of the security of unencrypted, computerized, personal information by persons doing business in the state. Includes an expanded list of sensitive personal information, including date of birth, mother's maiden name, employee ID number, and electronic signature. Exception for those financial institutions which are in compliance with federal guidance.

Rhode Island – H. 6191, enacted July 10, 2005, effective March 1, 2006, Requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons and by state agencies. Does not apply to HIPAA entities. Entities covered by another state or federal law are exempt only if that other law provides greater protection to consumers.

Tennessee – SB 2220, Passed into law in 2005, amends Tennessee Code Title 47 Chapter 18, Part 21, effective July 1, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Does not apply to persons subject to Title V of the Gramm-Leach-Bliley Act (financial institutions).

Texas – SB 122, Passed into law in 2005, effective September 1, 2005, Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons who conduct businesses in the state. Authorizes Attorney General to seek civil penalties for violations.

Washington – SB 6043, Signed May 10, 2005, effective in July 24, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons, businesses and government agencies. Notice is not required when there is a technical breach of the security of the system which does not seem reasonably likely to subject customers to a risk of criminal activity. Imposes civil liability for damages caused by failure to give notice as required.

Prepared by: Gail Hillebrand, West Coast Office, Consumers Union of US 415 431-6747

Appendix 3: Source, U.S. PIRG
State Security Freeze Laws

[These laws with links available at http://www.pirg.org/consumer/credit/statelaws.htm]

Update 19 September 2005

Enacted Security Freeze Laws:

California: ALL CONSUMERS Passed: September 2001; Effective: January 1, 2003.

Colorado: ALL CONSUMERS Passed: June 2005; Effective: July 1, 2006.

Connecticut: ALL CONSUMERS Passed: June 2005; Effective: January 1, 2006.

Illinois: IDENTITY THEFT VICTIMS Passed: June 2005; Effective: January 1, 2006.

Louisiana: ALL CONSUMERS Passed: July 2004; Effective: July 1, 2005.

Maine: ALL CONSUMERS Passed: May 2005; Effective: February 1, 2006.

Nevada: ALL CONSUMERS Passed: June 2005; Effective: October 1, 2005.

Texas: IDENTITY THEFT VICTIMS Passed: June 2003; Effective: September 1, 2003.

Vermont: IDENTITY THEFT VICTIMS Passed: June 2004; Effective: July 1, 2005.

Washington: IDENTITY THEFT VICTIMS, INCLUDING VICTIMS OF SECURITY BREACHES Passed: May 2005; Effective: July 24, 2005.

Security Freeze Bills that await gubernatorial action:

New Jersey: ALL CONSUMERS The New Jersey General Assembly has passed what will be the strongest security freeze law in the country. The bill allows all consumers to use the security freeze tool at minimal cost and requires the credit bureaus to facilitate the quick placement and lifting of the freeze. The Governor has committed to signing the bill. (EXPECTED TO BE SIGNED on 22 September 05)

North Carolina: ALL CONSUMERS.

Other states that considered freeze bills this year:

AK, CA, DE, HI, IN, KS, KY, MD, MA, MI, MN, MO, NJ, NM, NV, NY, OR, PA, TX, SC, UT