February
2004

Financial Privacy In The States

How Consumers Benefit From
Personal Information Safeguards

CALPIRG Education Fund

Financial Privacy In The States

How Consumers Benefit From Personal Information Safeguards

Dave Algoso
Steve Blackledge
Jasmine Vasavada

CALPIRG Education Fund
February 2004

Acknowledgments

The authors gratefully acknowledge the prior work of Ed Mierzwinski, Consumer Program Director of USPIRG, Vermont Assistant Attorney General Julie Brill, and Fordham University School of Law Professor Joel R. Reidenberg, whose research and advocacy have made this report possible. For generously giving their time to review the report, thanks also go to Gail Hillebrand of Consumer's Union, Susan Henrichsen of the California Attorney General's office, and Deirdre Cummings, MASSPIRG Consumer Program Director. Tony Dutzik, Ed Mierzwinski, and Susan Rakov of the State PIRGs contributed editorial assistance.

This report was made possible by the generous support of the Consumer Privacy Rights Fund of the Rose Foundation for Communities and the Environment.

The authors alone bear responsibility for any factual errors. The views expressed in this report are those of the authors and do not necessarily reflect the views of our funders.

The CALPIRG Education Fund is a nonprofit, 501(c)(3) organization that stands up and takes action when consumers are cheated and the voices of ordinary citizens are drowned out by special interest lobbyists. To encourage a fair, sustainable economy and foster responsive, democratic government, CALPIRG Education Fund conducts research, generates media attention, develops policy solutions, and educates the public.

CALPIRG Education Fund can be reached at:

1107 9th Street, Suite 601
Sacramento, CA 95816
(916) 492-1219

Additional copies of the report can be obtained by visiting www.calpirg.org.

Table of Contents

Executive Summary

Federal regulation riddled with loopholes has left large bank conglomerates and other financial institutions with too much leeway to share consumers' private information and too little responsibility for the consequences.

This report documents the growing concerns that Americans have about financial privacy, presents a survey of state laws that have helped fill regulatory gaps in the financial privacy sphere, and provides an estimate of the economic burden consumers currently bear as a result of inadequate privacy safeguards.

Misuse of Personal Financial Information Is a Growing Threat

- **The collection, selling and sharing of consumers' personal financial information for secondary commercial use has escalated as a result of a number of factors including:** industry consolidation; regulatory changes that have allowed banks, insurance companies, and other financial services to become affiliated through common ownership; and technological advances that have made the creation and distribution of massive consumer databases possible.
- **Financial institutions routinely profit by sharing and selling consumers' private financial information without their consent.** Last year, the financial services industry pocketed $937 million in California alone from the sale and sharing of consumers' private information, according to an analysis of data by the Direct Marketing Association.

Consumers Bear the Billion-Dollar Brunt of Inadequate Privacy and Security Protections

As a result of having inadequate privacy safeguards, we calculate a cost to consumers of $18.7 billion annually, or an average of $175 per household, in monetary outlays and lost time. (See tables on pages 26 and 27.)

- A recent survey by the Federal Trade Commission indicates that one in ten American adults (27.3 million) has been a victim of identity theft in the past five years, and nearly 10 million have been victims in the past year.
- Consumers lost more than $5 billion in out-of-pocket expenses and about 300 million hours of time (worth $4.6 billion at the current average hourly wage) last year due to these crimes, which overwhelmingly involve the misuse of personal financial information.
- One in six Americans say they have bought privacy protection services or products (at an estimated average cost of $75 annually) to avoid identity theft, check credit reports, or surf and shop online anonymously, fueling a growing national market estimated to be worth $2.5 billion annually.

Under current federal law, the average consumer has no ability to stop the sharing of his or her personal financial information among financial affiliates.

While relatively strong protections are in place to control how private information is used by other industries (including medical, cable television, and video rental), federal law passed in 1999 (the Financial Services Modernization Act, also known as Gramm-Leach-Bliley) allows financial institutions to share, sell, and otherwise use consumers' private

financial information without consumer knowledge, consent, or control. This law fails to implement the widely recognized Fair Information Practices, described below.

States Have Led the Way In Adopting Fair Information Practices As Law

Some states have led the way in ensuring consumers' personal financial information is protected by Fair Information Practices. These practices include:

Giving consumers access to and notification about data that is collected about them:

- In seven states (Colorado, Georgia, Maine, Massachusetts, Maryland, New Jersey, and Vermont), legislatures have made it easier for consumers to dispute and correct inaccurate data by providing them one free copy of their credit report each year, and some state laws require quicker reinvestigation and resolution of consumer disputes.
- Congress enacted similar legislation when amending the Fair Credit Report Act (FCRA) by passing the Fair and Accurate Credit Transactions Act (FACT Act) late in 2003. As a result, national credit bureaus must provide free reports upon request within 15 days of the request. States are preempted from increasing the frequency of the provision of free reports (free report laws in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont are "grandfathered").

Giving consumers control over how their personal information is used:

Opt-in: Vermont and Alaska have adopted laws that require financial services companies to obtain express consent from the consumer before they may share private information with affiliates or third parties (with some exceptions). Alaska, California, Connecticut, Florida, Illinois, and Vermont have extended consumers the right to opt-in for information sharing with third parties only.

Opt-out: California law also empowers consumers to choose not to have their information shared with financial affiliates. The FACT Act also made permanent the federal preemption in FCRA against states regulating the sharing of information among affiliates. However, the interplay between this provision and the federal Gramm-Leach-Bliley Act, which specifically authorizes state action, has not been determined and is likely to be addressed through future court rulings.

Giving consumers the legal ability to correct errors in their personal data files and obtain redress from data furnishers if their information is misused or is inaccurate:

- California and Massachusetts have adopted stronger-than-federal laws increasing liability of data users and furnishers for inaccurate data they provide to credit bureaus or use in credit decisions.

Giving consumers other rights to ensure against the misuse of their data:

- California requires collectors of computerized data to notify any individuals whose data may have been acquired by an unauthorized person.
- Starting January 1, 2005, California consumers may request that a business disclose the details of information shared with third parties, and the business must comply or provide the consumer a cost-free means to opt out of all future sharing.

States and Companies With Strong Privacy Protections Can Do Good While Doing Well

Industry research has argued that protecting privacy may have negative economic impacts. While a comprehensive economic analysis is beyond the scope of this report, several indicators contradict these claims:

- When compared with other states, “opt-in” states and states with added responsibility for data furnishers experienced lower average bankruptcy rates and lower average mortgage interest rates.
- One survey of financial services institutions (including community banks and credit unions in addition to the largest national banks and credit companies) has shown that up to 25% of these institutions currently operate without selling or sharing their customers’ information.

Introduction

Americans today are more concerned than ever about their privacy, and there is good reason.

New technology and changes in the retail marketplace have increased the amount of information consumers leave behind as they go about their business. Supermarket scanners and online retailers collect vast amounts of information about consumer preferences, while Web surfers leave a trail of their medical, political, and recreational interests wherever they go on the Internet.

Also, banks, insurance providers, credit providers, and brokerage firms are increasingly likely to operate under one roof because of recent changes in federal law. Companies that are connected through common ownership—known as "affiliates"—have increased latitude to share consumer records of medical payments, charitable contributions, life insurance and healthcare usage, retirement assets, and other financial transactions.

Finally, technological advances have enabled firms to collect, analyze, and disseminate more consumer information at lower cost and faster speed than ever before.

As a result of these three changes—all of which have occurred within just the last decade—more information that consumers once held as private is in circulation among businesses, which have both greater ability and greater incentive to exploit that information.

The secondary use of a consumer's most private information to compile profiles assist efforts to market goods to that consumer, without the consumer's express consent, comes at a price. The price ranges from the momentary inconvenience of a telemarketing call in the middle of dinner to the months-long nightmare of restoring one's good name after critical information falls into the wrong hands and is used in an identity theft.

With identity theft skyrocketing, commercial use and abuse of consumers' personal information at an all-time high, and federal protections riddled with loopholes, state policymakers are stepping in to fill the void. Across the nation, states have passed legislation empowering consumers with greater control over how their sensitive personal information is used upon entering the electronic world of data transfer. In so doing, states are fulfilling their traditional role as "laboratories of democracy"—using innovative new strategies to deal with this growing social problem.

Lack of Privacy Harms Consumers

In passing consumer privacy protections, state legislatures have responded to a public outcry that has grown significantly over the past decade. This outcry has its roots in strong consumer sentiment that individuals should have the right to control how and where their personal information is used, and that this information is increasingly ending up in the wrong hands.

Polling data show that since 1990, the average consumer has become much more wary about voluntarily yielding his or her personal information to a business or company. In a 1998 poll by Harris and Associates, more than 3 in 4 people (78%) reported that they had refused to give information to a business or company because they deemed it not necessary for the transaction or too personal. This represents a stark increase from 1990, when fewer than half of people surveyed (42%) reported ever having refused to share information.[1]

This demonstrates that when consumers have control of whether or not to share information, they increasingly are deciding not to do so. However, all too often, information is being collected and shared in ways consumers may not suspect and have very little control over.

Consumers report widespread privacy abuses

In the same 1998 poll, 41% of respondents (representing 78 million adults) reported that they had *personally* been the victims of an improper invasion of privacy by a business.[2]

Personal financial information may be exploited in a number of ways:

- **Intrusion**: unwanted mail or telemarketing;
- **Manipulation**: secondary use of the data in a marketing profile that enables "hidden persuasion." This concern is especially strong for vulnerable groups such as the elderly;
- **Discrimination**: use of personal information in creating secret standards or profiles for making consumer risk-assessments;[3]
- **Fraud and identity theft:** criminal use of an individual's personal financial information to make purchases, open new accounts, or otherwise misrepresent one's identity.

Without better safeguards in place, consumers' personal information is increasingly likely to end up in the wrong hands, leaving consumers vulnerable to one of the fastest growing crimes in the nation—identity theft.

Manipulation, Discrimination, and Consumer Fraud

One of the most egregious ways in which a bank or its affiliates can use personal financial information is to exploit vulnerable or less-knowledgeable individuals for riskier investments, based on the sharing of their financial histories.

Sharing of personal financial information without consent facilitated abuses by NationsSecurities, an affiliate of NationsBank (now known as Bank of America). In the early 1990s, according to court documents, NationsSecurities sales staff misled unsophisticated investors into believing that they were dealing with bank employees and that their money would be invested in insured bank products, rather than risky over-the-counter derivatives. A number of elderly investors lost much of their life savings.[4] In this case, the SEC issued a cease-and-desist order to stop the fraudulent practices.

In September 2002, CitiFinancial was ordered to pay fines of $215 million in consumer redress for "deceptive practices." In a court declaration in this case, brought by the Federal Trade Commission, a former assistant manager described the standard practices of using personal financial information to target vulnerable consumers:

"I and other employees would often determine how much insurance could be sold to a borrower based on the borrower's occupation, race, age and education level. If someone appeared uneducated, inarticulate, was a minority, or was particularly old or young, I would try to include all the coverages CitiFinancial offered."[5]

Financial institutions also betray consumer trust when they share account information with third parties for use in "pre-acquired account telemarketing." This practice increases the potential for unauthorized charges by providing telemarketers with information necessary to bill consumers at the time a telemarketing call is made.

In June 1999, US Bancorp agreed to change its information sharing practices as part of a settlement with the attorneys general of 38 states and the District of Columbia. The lawsuit alleged that the bank had disclosed the names, phone numbers, social security numbers, account balances, and credit limits of almost one million customers to an unaffiliated company called MemberWorks. The bank was charged with misrepresenting its privacy policies, because it told its customers "all personal information you supply to us will be considered confidential." MemberWorks had called US Bancorp customers and offered them 30-day "free" trial memberships in discount programs. Many of the customers thought the trial period was a safe bet because they never gave MemberWorks their account numbers or authorization to charge them; the customers did not know that MemberWorks already had already gotten their account numbers from their bank, and would charge them at the end of the 30 days unless the customer actively took steps to cancel the membership. US Bancorp received $4 million plus commissions on sales made by MemberWorks. MemberWorks also settled the suit.[6]

In January 2000, Chase Manhattan Bank agreed to change its information sharing practices as part of a settlement with the New York Attorney General's office. Chase Manhattan Bank had provided nonaffiliated third party vendors with bank customers'

names, addresses, phone numbers, and account information, including encrypted account numbers and credit usage history (for example, credit line, current balance, how long the customer has had the card, and the date of the last transaction). In exchange, Chase received a fee if customers purchased a product or service from the vendor. The Attorney General's office charged Chase with not fully and adequately disclosing to its customers what information would be provided to non-affiliated third party vendors, and with not informing its customers of their ability to prevent such information from being provided.[7]

In December 2000, the Minnesota Attorney General's office filed suit against Fleet Mortgage for a similar practice. As part of joint-marketing agreements, Fleet had provided telemarketing companies with customers' names, addresses, phone numbers, and loan account numbers, and sometimes also with specific information on the terms of the loans. Customers were subject to deceptive telemarketing practices similar to those of MemberWorks, though in this case the financial institution itself stood accused of the abuse. Fleet settled the lawsuit and agreed to pay restitution.

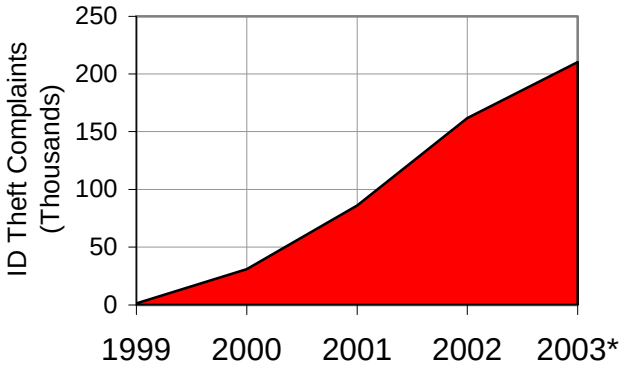
Each of these abuses eventually found resolution, though only with much headache for consumers and hard work by various state Attorneys General. These deceptive practices would not have been possible in the first place were it not so easy to play fast and loose with private financial information.

Identity theft is skyrocketing

With the creation of massive databases and a lack of adequate safeguards in place to protect personal information, consumers are increasingly victims of identity theft—a crime in which sensitive information is illegally used to commit fraud.

The threat of identity theft has escalated rapidly in the past decade. Figure 1 depicts how identity theft reports to the Federal Trade Commission's (FTC) Consumer Sentinel database have increased more than four-fold in the past four years.[8] Furthermore, a recent survey by the FTC shows that ID theft reported to the Consumer Sentinel may be just the tip of the iceberg. This survey, which randomly sampled 4,057 Americans, shows that approximately 1 in 8 American adults (27.3 million) have been victims of identity theft in the past five years, and in the last year alone almost 10 million have discovered that they were victims.[9]

Figure 1. Identity Theft is Skyrocketing



*(2003 projected based on complaints registered in first half of year)

The cost of these crimes is significant. The FTC study found that last year, identity theft cost victims $5 billion in out-of-pocket expenses and cost businesses nearly $48 billion.[10]

While estimates vary, studies have documented that victims must spend a great deal of their own time and money getting their records cleared. A 2000 joint study by CALPIRG and the Privacy Rights Clearinghouse found that ID theft victims reported an average of $808 in personal expenses and 175 hours in lost time resulting from abuse of their private information.[11] In 2003, using a similar survey methodology, the Identity Theft Resource Center documented an increase in these factors—from $808 to $1495 in out-of-pocket expenses and from 175 to 607 hours.[12]

When an identity thief creates new accounts in a victim's name, such as credit card or utility accounts, victims have an especially difficult time. In the 2003 FTC poll, victims of these "new accounts frauds" reported spending an average of 60 hours and $1,200 in out-of-pocket expenses getting their names cleared.[13] They experience harassment by debt collectors (35% of victims) and find their credit record in shambles, leading to higher interest rates or even loan rejections (35% of victims); some are even sought by law enforcement officials when a thief commits other crimes under the stolen identity (14% of victims).[14]

The above estimates, of course, ignore the emotional damage caused by identity theft crimes, such as: a sense of powerlessness or helplessness, reported by 76% if ID theft victims, and sleep disturbances (unable to sleep, oversleeping, nightmares) reported by more than half of ID theft victims.[15]

Identity theft usually involves misused financial information

The 1999 Gramm-Leach-Bliley Act loosened restrictions on common ownership among banks and other financial institutions, leading to an increased flow of information as banks share information with "nonbank affiliates" or sell information to third party retailers who target products to their customers.

Unrestrained information flow can increase a company's profits, but makes a customer's personal information accessible to more parties. This wide availability has made identity theft easier, and the electronic storage of sensitive information in an increasing number of places makes thieves difficult to track down.

Much of the time, identity theft involves misused financial information. The recent FTC survey found that 85% of identity theft cases involve the misuse of one or more of the victim's existing financial accounts (such as credit card, cell phone, or utility accounts.)[16]

In fact, nearly one in four identity theft victims who learn the identity of the perpetrator report that it was a person working for a company or financial institution that had access to the victim's personal information.[17]

One reason identity theft may be so widespread is that companies do not have economic incentives to institute measures to prevent the crime, given the profit incentives to banks, department stores and other companies from using and selling consumer data combined with insignificant liability when the personal information held by the company is misused or abused.

A lack of liability for the damages resulting from fraud and identity theft, most of which fall on the consumer, can lead to a lack of incentive for corporations to take adequate preventive measures. Only 26% of victims become aware of the crime due to proactive steps taken by a financial institution or other business.[18] Many victims also report frustration over dealing with credit bureaus and lenders to get their records cleared of the fraud's negative effects.

Lack of safeguards creates opportunities for insider fraud

Several cases have been documented in which employees in financial service institutions abused their access to customer information:

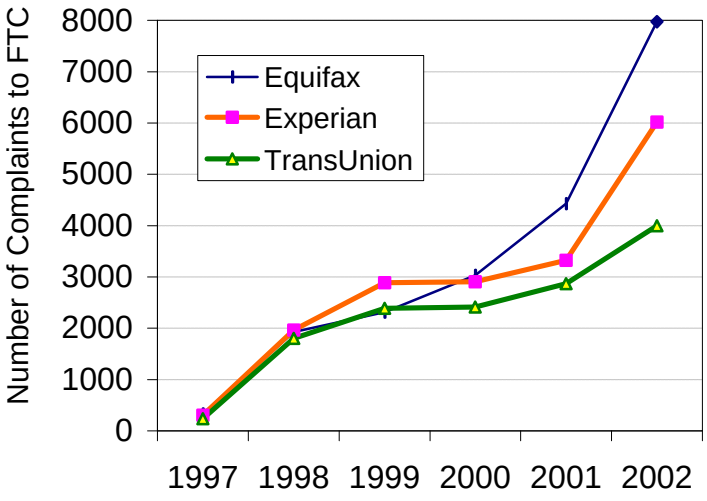
In February 2003, a former First USA Bank employee pleaded guilty to stealing customer account information that was then shared with an accomplice who used the information to make purchases.[19]

In October and November 2002, federal prosecutors charged three men with stealing the personal financial information of 30,000 people over three years and selling it to scam artists for $60 per name. One of the men was a computer help-desk worker at Teledata Communications Inc., a company that helps lenders access the major credit data repositories.[20] The man was able to use his laptop to access private data, and the fraud continued, even after he stopped working for the company.[21]

In July 2002, ten credit card and bank employees were charged with identity theft or related financial crimes.[22]

In 2000, two Delaware men pleaded guilty to running fraud rings in which they paid employees of financial companies for account information, including credit card numbers, dates of birth, social security numbers and home addresses from Discover Card employees. [23]

Figure 2. Rising Consumer Complaints About Credit Bureaus



Consumers want companies to protect their private information

In poll after poll, consumers overwhelmingly support strong privacy protections. In fact, nine out of ten Californians surveyed by the Consumer Federation of California stated that they would vote in support of an initiative that extended stronger privacy protections to consumers.[24]

This is unsurprising when one considers that most Americans feel that they have a right to know what information is collected on them and by whom, and furthermore that they should have control over that information. Most people feel that they do not currently have adequate control over their personal information.

Nationwide polls have documented that:

- 97% of Americans feel that it is important to be in control of who can get information about them.[25]
- 93% feel that it is important to be in control of what information is collected about them.[26]
- Concern about companies sharing information with other companies without consumer consent (75%) is even stronger than concern about transactions being insecure (70%).[27]
- More than two-thirds (69%) of those surveyed feel that consumers have lost all control over how information is collected and used by companies.[28]
- Less than half (44%) feel that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.[29]
- Less than half of those surveyed (42%) feel that most businesses handle personal information they collect about consumers in a proper and confidential way.[30]

Consumers rank financial privacy highest in importance

A February 2002 Harris Interactive poll showed that consumers are deeply concerned about protecting their financial information. More consumers ranked "financial services" industry privacy protections as very important than any other industry, including health care.[31]

Percent of respondents ranking effective privacy protections "Very Important":

1. Financial services	85%
2. Health care providers/pharmacies	74%
3. Telecommunications	57%
4. Retail and travel	37%
5. Entertainment/subscriptions	28%

Financial privacy concerns often center around access to and sale of personal financial information

A poll for USA Weekend, conducted by the Opinion Research Corporation in July 2000, found that 84% of adults say too many people have access to their credit report, and 79% say too many people have access to their financial records.[32]

A January 2002 poll, conducted by the Evans McDonough Company for online lender E-LOAN, found that 82% of California voters view protecting the privacy of their financial information as a critical concern; 80% also said they are not at all comfortable with financial institutions selling their personal information.[33]

What Personal Information Can Be Sold and "Shared" by Your Financial Institution?

Financial information is highly personal information—information consumers rarely share with friends, neighbors, and extended family, much less strangers. Yet this information is collected in databases that are sold to the highest bidder and shared with affiliates, and may include "transaction and experience" data such as the following[34]:

- details of your credit card, debit card, and personal check use. Such details may include records of your purchases, including where you eat or shop, how much you spend there, and even what kinds of things you buy. Banks now have the technology to scan information off your checks;
- the size of your account balance(s);
- the names of co-owners of those accounts;
- the frequency and size of your deposits;
- your projected net worth based on accounts with them;
- your payment history on loans;
- your finance charges; and
- your current and historic debt levels.

All this experience and transaction information can be shared with either affiliates or third parties involved in joint marketing agreements with the bank—even if consumers request that this information remain confidential.

Fair Information Principles Are the Basis for Strong Privacy Protections

Safeguarding personal information is no small task in a world where the quantity of information that can be stored and transmitted doubles every eighteen months--a world in which such information is highly sought-after by a broad range of commercial and industrial interests.

The Organization of Economic Cooperation and Development (OECD) established the international standard for the use of personal data in 1980. Their guidelines involve eight principles:

1. **Collection Limitation**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification**: The purposes for which personal data are collected should be specified at or before the time of data collection.
4. **Use Limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law.
5. **Security Safeguards**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Consumers should be able to readily determine what is collected about them, by whom, and for what use.
7. **Individual Participation**: An individual should have the right:
    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
    c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability**: A data controller should be accountable for complying with measures that give effect to the principles stated above.[35]

These principles are generally referred to as Fair Information Practices, or FIPs. They echo and amplify principles laid out in the early 1970s by the U.S. Department of Health,

Education and Welfare as it faced the problem of developing a system to store personal medical information that would reap the benefits of computerization while maintaining critical safeguards to ensure sensitive information would not be misused.

The FIPs undergird key laws on information sharing. The Privacy Act of 1974, for example, outlined ways in which the government should be restricted from using private information. Relatively strong laws also exist in areas such as medical information, student records, video rentals, and more.

While the 1970 Fair Credit Reporting Act is largely based on applying the FIPs, it has not kept up with the growth in information sharing practices. The 1999 Financial Services Modernization Act (widely referred to as the Gramm-Leach-Bliley Act) is, at best, based on a heavily watered-down version of the FIPs. While the law technically requires banks and credit institutions to notify consumers of how their data will be used, in practice, these notices are so poorly and technically written that few consumers reading them would be adequately informed about the bank's actual practices. Furthermore, it fails to give consumers the right to inspect their comprehensive personal profiles, correct these files, or control their use for secondary purposes.

Federal regulation of consumer privacy: protections and preemptions

The 1996 Fair Credit Reporting Act amendments and the 1999 Financial Services Modernization Act, commonly known as the Gramm-Leach-Bliley Act (GLBA), create the current federal regulatory framework for financial privacy law.

The 1996 FCRA amendments allow affiliated companies to share "transactions and experience" information. This can include detailed information about purchases made with a credit card, outstanding account balances, and payment history. Consumers have no way to stop this sharing under FCRA.

On the other hand, the 1996 FCRA amendments give consumers the ability to stop, or opt out of, the sharing of what is known as "other" information with affiliates. "Other" information is what the customer provides to the company, for example from an application, a credit report, or references. It can include credit scores and history, employment history, marital status, medical history, and information from a credit application (including income information). Consumers can also opt out of prescreened credit offers.

The primary function of GLBA is to allow for unprecedented mergers and common ownerships among banks, insurance companies, securities firms, and other financial services companies. More affiliation inevitably means more information sharing and increased access to consumers' personal information. The privacy protections offered under GLBA are seriously incomplete—only giving consumers the ability to opt out of having their information shared with unaffiliated third-party companies that market nonfinancial products. Companies would still be able to share or sell customer information freely with other third parties, for example under joint marketing agreements. They also must inform customers of their right to opt out.

One of the most important provisions of GLBA explicitly gives states the right to enact privacy protections stronger than those in federal law. Known as the Sarbanes amendment, this provision allows states to serve as laboratories of democracy, enacting stronger privacy reforms.

The 1996 FCRA amendments also included a temporary preemption of some state laws. These preemptions were made permanent when Congress passed the Fair and Accurate Credit Transactions Act (FACT Act).[36] The expiration was widely debated in Congress, and the financial services industry mounted a fierce and effective campaign to make those preemptions permanent. Yet, several stronger state laws governing fair credit policy —in Vermont, California, and Massachusetts—predate both the 1996 FCRA amendments and the FACT Act. These were "grandfathered" and remain exempt from the preemption to date.

Financial services companies argued to extend the preemption of state laws, supporting a uniform national standard in place of the current "patchwork" of privacy policies. They support one national standard even in cases where privacy protections currently enjoyed by consumers in some states would be lost as a result.[37]

On the other hand, state Attorneys General and others have argued that state governments serve as important laboratories for developing consumer protections, nimble enough to respond quickly and small enough to risk innovation. In consumer protection, as in other issue areas, states have served as incubators of creative reform. The patchwork of laws that financial institutions worry about has frequently made the overall regulatory framework stronger.

State Privacy Protections

States have proven nimble players in helping to fill the regulatory void created as technological advances in information sharing have surpassed legal safeguards established by the federal government. States have developed a range of protective policies intended to help consumers maintain the integrity of their "financial DNA"—private financial information—in the Information Age.

Use limitation principle

Consumers should have the right to control how their private information is used, and to decide if their personal financial information is used for secondary purposes, whether by affiliates of a financial institution or third parties. People should be able to choose for themselves whether the possible benefits of information sharing are worth the risks.[38]

Opt-in and Opt-out: Who really has control?
Policies that aim to give consumers ultimate control over whether their information is shared in a particular instance are either opt-in or opt-out. Because of the difficulties with implementing the systems and disincentives for financial services companies to make them effective, however, only opt-in systems provide consumers with actual control over their information.

Under **opt-in**, a company is not allowed to share the consumer's information unless it has gotten the affirmative consent of the consumer. If the consumer has expressed no opinion, the default is that the company is forbidden from sharing the information.

Under **opt-out**, a company is allowed to share the consumer's information until the consumer objects. If the consumer has expressed no opinion, the default is that the company is allowed to share the information.

If People Care About Privacy, Why Don't More People "Opt Out"?
Financial institutions frequently point to the fact that very few people opt out of information sharing as evidence that privacy is not important to consumers, despite polling data that shows otherwise.

A 2001 study by the Privacy Rights Clearinghouse demonstrated that notices on privacy policies—which, under current federal law, financial institutions must send to customers to inform them of their ability to opt-out—are frequently written in a manner that makes the policies difficult to understand.[39] The study analyzed the readability of privacy notices from 60 major financial institutions, finding that the average notice required a 3rd-4th year college reading level, far beyond the junior high level that literacy experts recommend for communicating with the general public. Separate recent studies by CALPIRG (*Privacy Denied: A Survey of Bank Privacy Policies,* August 2002)[40] and USAction[41] have similarly demonstrated the inadequacy of bank privacy policies.

In fact, one banking industry journal acknowledged that privacy notices do not reflect what legislators and the public demanded. In an October 2001 issue of *American Banker*, one article noted: "Unfortunately, as a means of conveying an institution's commitment to protect consumer privacy, a legally compliant Gramm-Leach-Bliley privacy notice is woefully inadequate."[42]

Despite federal requirements that financial institutions give consumers the ability to opt out of third party sharing, there is disincentive for these institutions to make the process easy or understandable. Sharing consumer information with their affiliates gives companies a financial "leg-up" on the competition, and third parties often pay companies for their customer lists.

Potentially, privacy notices and opt-out clauses could work better, if they were written by consumer advocates rather than private companies, and enforced by regulators with stiff penalties for non-compliance. However, as currently implemented, opt-out policies do not effectively empower consumers with control of their personal information.

Sharing of insurance information-
The following states have opt-in rules for disclosure of personal information by insurance companies:

- Arizona (Ariz. Rev. Stat. § 20-2113)
- California (Cal. Ins. Code § 791.13)
- Connecticut (Conn. Gen. Stat. § 38a-988)
- Georgia (Ga. Code § 33-39-14)
- Maine (Me. Rev. Stat. 24-A, § 24-2215)
- Massachusetts (Mass. Gen. Laws 175I, § 13)
- Minnesota (Minn. Stat. § 72A.502)
- Montana (Mont. Code § 33-19-306)
- New Jersey (N.J. Perm. Stat. § 17:23A-13)
- New Mexico (N.M. Admin. Code § 13-1-3)
- North Carolina (N.C. Gen. Stat. § 58-39-26)
- Ohio (Ohio Rev. Code § 3904.13)
- Oregon (Or. Rev. Stat. § 746.665)
- Vermont (Vt. BISHCA Reg. IH-2001-02)

Sharing by financial institutions-
The following states have laws that restrict financial institutions from certain types of information sharing with affiliates and unaffiliated third parties:

- Alaska: opt-in for affiliate and third-party sharing, with some exceptions (Alaska Stat. § 06.01.028)
- California: opt-out for some affiliate sharing, opt-in for third party sharing (SB 1, chaptered 8 August 2003, effective 1 July 2004)
- Vermont: opt-in for all third-party sharing; opt-in for affiliate sharing of information that is not "transactions and experience" information; no control over "transactions and experience" information (Vt. Stat. Ann. tit. 8 § 10203-10204; tit. 9, § 2480e)

The following states have more limited opt-in laws that restrict sharing only with third parties:

- Connecticut: opt-in for third-party sharing (Conn. Gen. Stat. §§ 36a-41, *et seq*.)
- Florida: opt-in for third-party sharing (Fla. Stat. § 655.059)
- Illinois: opt-in for third party sharing (Ill. Comp. Stat. Ann. Ch. 205 § 5/48.1)
- North Dakota: opt-in for third-party sharing (N.D. Cent. Code § 6-08.1)

The North Dakota Story

Strong support for privacy protections is clearly reflected in North Dakota. The state's small population of 650,000 makes it an ideal laboratory for democratic reforms reflecting consumers' policy priorities.

On June 11, 2002, a groundswell of grassroots support for strong privacy protections culminated in the passage of a referendum in which North Dakotans voted 3-to-1 in favor of restoring important privacy protections to consumers in the state—repealing a state law that had granted banks and financial institutions the right to sell customer information without first obtaining permission.

The history of financial privacy laws in North Dakota has been tumultuous, starting with a 1985 law that prohibited banks and financial institutions from sharing customer information even with affiliated companies. This strong law put the state ahead of its time for protecting consumers. Under pressure from the North Dakota Bankers Association, the state's law was amended in 1997 to allow for affiliate sharing. This change gained in significance two years later, when the federal Gramm-Leach-Bliley Act (GLBA) loosened barriers between common ownership of banks and other financial institutions.

In 2001, state lawmakers passed Senate Bill 2191, replacing North Dakota's opt-in law for third-party sharing with a less protective opt-out policy. Lobbyists for the banks and credit unions had argued the bill was necessary to bring the state into compliance with federal law, and warned lawmakers that not passing the bill would result in job losses and negative economic development.

SB 2191 went into effect in July 2001, but within six weeks, a grassroots effort calling itself "Protect Our Privacy" collected over 17,000 signatures supporting a referendum to repeal it. Despite a special interest advertising campaign that outspent the grassroots effort 8-to-1, the people of North Dakota overwhelmingly voted to restore financial privacy protections by repealing SB 2191.

California Takes on Affiliate Sharing

In 2002, several California municipalities (San Mateo County, Contra Costa County, and Daly City) passed ordinances establishing opt-in rules for sharing with both affiliates and non-affiliated third parties. In response to a lawsuit filed by Bank of America and Wells Fargo, a federal judge struck down the restriction on affiliate sharing on July 29, 2003, but the restriction on third-party sharing was upheld.[43]

In August 2003, the California Legislature passed Senate Bill 1, a law touted as "the strongest financial privacy law in the country." This law gives consumers the ability to opt out of information sharing with affiliated companies, and sets an opt-in standard for many third party uses. Such policies have become important in an era in which major national banks like CitiCorp and Bank of America have hundreds of affiliates in their corporate families with whom they can share private information.

Security safeguards principle

California law requires that, in the event of a security breach, anyone who owns or licenses computerized data that includes personal information notify Californians whose data may have been acquired by an unauthorized person. (Cal. Civ. Code §§ 1798.29, 1798.82)

Openness principle

Starting on January 1, 2005, California law will require a great deal more openness about information sharing practices. California Senate Bill 27, passed and signed in September 2003, requires nonfinancial businesses to disclose to a customer, upon request, the details of information shared with third parties or to provide the consumer a cost-free means to opt out of all future sharing. Information disclosed includes details of the sources and recipients of that information, and in many cases, copies of the information that was disclosed.

Individual participation principle

When records are kept on an individual, that person has a right to know what information is being collected and how it will be used. Federal law has helped in this area, but states have gone even further to protect citizens' rights to access the records kept on them. Furthermore, when a record contains errors that might result in adverse actions, the consumer has a right to correct the mistakes. The process should be simple and accommodating. This is especially important for minimizing the harm done by identity thefts.

Free credit reports- Under federal law, anyone who has reason to believe that his or her credit report contains inaccurate information as a result of fraud or identity theft is entitled to a free credit report. The following states go the next step by allowing *all* consumers at least one free copy of their credit reports every year:

- Colorado (Colo. Rev. Stat. §§ 12-14.3-101, *et seq.*)
- Georgia, two per year (Ga. Code § 10-1-393(b)(29))
- Maine (Me. Rev. Stat. Title 10, § 10-1316, as revised by Public Law Chapter 118, effective 13 September 2003)
- Maryland (Md. Code Com. Law § 14-1209)
- Massachusetts (Mass. Gen. Laws ch. 93 § 56)
- New Jersey (N.J. Stat. § 56:11-37)
- Vermont (Vt. Stat. Title 9 § 2480b)

California allows credit bureaus to charge up to $8 for file preparation, which must be waived if the consumer has been a victim of identity theft. This law also requires that all information in the file be disclosed, including how the credit score is calculated and the credit score itself, in some circumstances (Cal. Civ. Code §§ 1785.11.1, 1785.15.1, 1785.19). The Colorado free credit report law contains a similar provision. Another California law provides victims of identity theft with 12 free credit reports over the course of one year (Cal. Civ. Code §§ 1785.15.3).

Investigation- California law requires that a consumer reporting agency reinvestigate, free of charge, any dispute made by a consumer of any item of information in the consumer's file. Also, upon notice of dispute by a consumer reporting agency, a furnisher of information must reinvestigate disputed information upon notice by a consumer reporting agency. (Cal. Civ. Code § 1785.16)

The Credit Score Lottery

Any system that attempts to keep records on millions of people is bound to contain some errors. Inaccurate data in the credit reporting system, however, can cost consumers thousands of dollars.

A February 2003 Federal Reserve Bulletin, for example, noted that about 70% of the reports in a study sample had a missing credit limit on one or more of the consumer's revolving accounts, resulting in "a higher estimate of credit utilization and probably a higher perceived level of credit risk for affected consumers"—in other words, raising consumer rates artificially.[44]

In 2002, the Consumer Federation of America analyzed the credit scores of more than 500,000 consumers from all three major credit repositories (Experian, Equifax, and TransUnion).[45] They found that the three data repositories often gave very different scores for a given person: 29% of consumers had scores that ranged more than 50 points, and 4% had scores that ranged more than 100 points. Credit scores usually fall between 400 and 800, with 620 being a common cutoff point for prime rates.

The study also looked more closely at a group of consumers whose scores were such that their ability to get prime rates may be affected by errors in their credit history. Comparing the records from the different data repositories, two-fifths of these "at-risk" borrowers' records were found to contain errors that would affect the credit rates they are offered. One-fifth had errors that would help their ability to get credit, while one-fifth had errors that would harm their ability to get credit.

In the aggregate, this works out for a lending institution. One-fifth of the time, a consumer is offered a worse rate than she deserves, and the company is not taking as big a risk as it thinks. One-fifth of the time, a consumer is offered a better rate than she deserves, and the company is taking a bigger risk than it thinks. Statistically, these risks balance out for the company. For the individual consumers, however, it becomes a matter of luck.

The Consumer Federation of America uses a hypothetical consumer who is incorrectly placed into a 9.84% "A-" loan on a 30 year, $150,000 mortgage.[46] This consumer would pay $317,516.53 in interest. With the 6.56% prime loan that this consumer should have gotten, the interest payments would have been $193,450.30. This consumer would pay $124,066.23 too much over the lifetime of the loan.

The report states the problem succinctly: "Credit scores should not function as a lottery in which some consumers 'win' by being viewed more favorably than they deserve to be, while others 'lose' by being viewed less favorably than they should be."[47]

Freezing access to credit file- California and Texas both have laws that allow consumers to "freeze" their credit reports. Consumer reporting agencies cannot release any information from a consumer file that is frozen. This helps solve the problem of lenders ignoring fraud alerts in identity theft victims' reports, which federal law requires credit bureaus to place upon consumer request. (California Civil Code § 1785.11.2; Texas Senate Bill 473, effective 1 September 2003).

Accountability principle and data quality principle

Any company or organization that collects, uses, or shares identifiable personal data should be responsible for ensuring that the data is accurate and used only for the intended purposes. This means stronger responsibilities and liabilities for furnishers and users of information.

Liability- Massachusetts law requires that furnishers of information establish reasonable procedures to ensure accuracy of data reported, and holds them liable for reporting information they know or should know is inaccurate. (Mass. Gen. Laws ch. 93, § 54A(a))

Notification- California law requires that a furnisher of information notify a consumer when negative information is provided to a consumer reporting agency. (Cal. Civ. Code § 1785.25(a))

The Economics of Privacy Protections

There is reason to believe that, by inspiring consumer confidence and helping to guarantee the quality of consumer data contained in credit reports and other databases, state privacy laws not only benefit the consumers they are designed to protect but also go hand in hand with successful businesses and robust economic indicators.

State privacy protections are linked to positive consumer indicators

Each state's average mortgage rates and the number of bankruptcies per household can be used as proxies to indicate whether financial privacy policies have had a noticeable impact on the state economy.[48] Indeed, the financial services industry has argued that credit decisions would be adversely affected by information sharing policies, potentially affecting these consumer rates with significant harm to consumers.

Financial institutions have argued that financial privacy policies may have a "chilling" effect on the collection of data for the credit system. Since this system relies on detailed data repositories to make rapid decisions about a consumer's credit-worthiness, the argument goes, any laws that potentially restrict the flow of some consumer information may then result in higher rates and restricted access to credit for consumers. These sorts of laws include:

- "Opt-in" laws in which consumers can choose not to allow sale or sharing of their personal information to third parties and/or affiliates (currently in place in Alaska, California, Connecticut, Illinois, North Dakota, and Vermont);
- Laws that increase responsibilities of data furnishers, such as increasing liability for furnishing inaccurate information or requiring furnishers to notify consumers when negative information is provided (currently in place in Massachusetts and California).

Since credit mortgages account for over 70% of consumer borrowing, an analysis of effective mortgage rates, which include fees and charges, can give an indication of the cost to lenders of extending credit. Bankruptcy rates provide an indication of how frequently non-creditworthy consumers are extended credit, and thus they indicate whether lenders are able to make good decisions regarding credit risks.[49]

Our comparison of these two indicators in the states identified above versus the national average suggests that adoption of strong privacy policies, if anything, may positively impact state economies and consumer rates.

State financial privacy policy impacts on mortgage rates

The average effective mortgage rate for the eight privacy states last year was 6.46%, compared to a national average of 6.59%, a difference of 0.13 percentage points. Over the last five years, the average rate in privacy states was 7.16%, compared to 7.24% in all other states, a difference of 0.08 percentage points. See figure 3.[50]

Figure 3. Effective mortgage rates: States with strong privacy protections compared to others

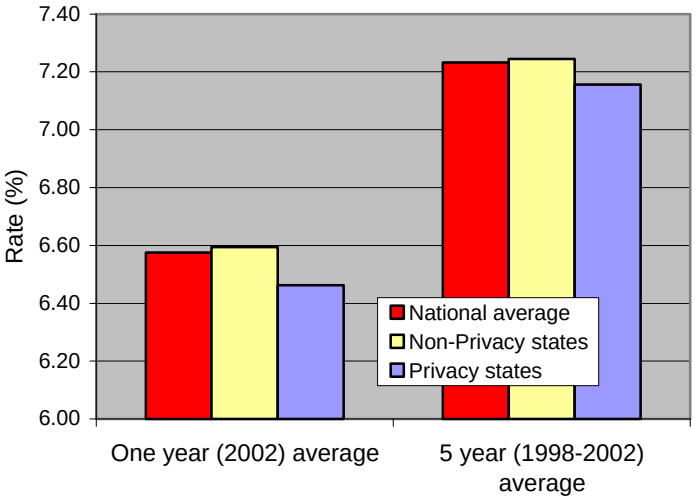
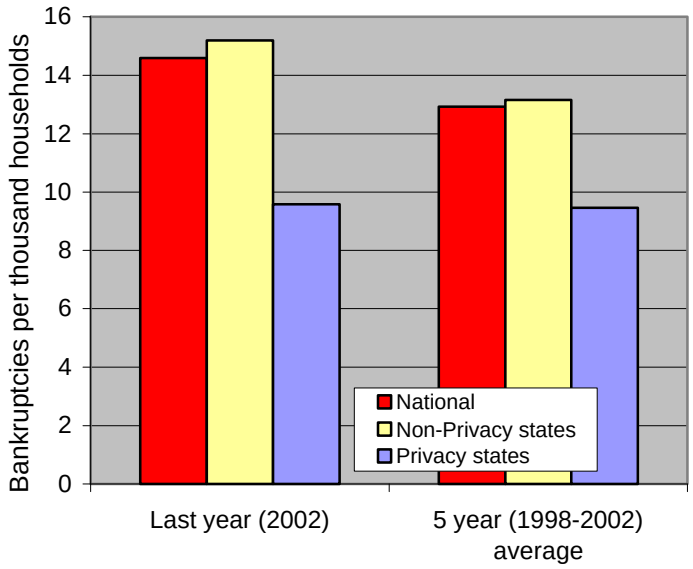


Figure 4. Bankruptcy rates: States with strong privacy protections compared to others



State financial privacy policy impacts on bankruptcy rates

The frequency of bankruptcies last year for the states with increased responsibilities of furnishers was well below the national rate. Most of the states with various opt-in laws are also well below the national rate. The number of non-business bankruptcies filed per thousand households in the privacy states last year was 9.58, and averaged 9.46 over the last 5 years. The rate for all other states last year was 15.19, and averaged 13.15 over the last 5 years. See figure 4.[51]

There are obviously many factors involved in mortgage rates and bankruptcy rates, making it impossible to conclude that strong privacy protections lead to fewer bankruptcies or that greater responsibilities of furnishers lead to lower mortgage rates. It is clear, however, that if there is a correlation, on average it seems that privacy states are doing quite well in both of these areas compared to other states.

An additional benefit of many privacy laws: improving quality of data
Laws that increase liability of data furnishers for mistakes and increase consumer access to their credit reports do more than restrict information flow—they help restrict the flow of *inaccurate* information, information that not only harms consumers, but harms creditors' ability to make good decisions.

This raises an important point—that quantity of data availability is not the only significant factor. In many cases, the quality of the data is just as important. Indeed, incorrect data can do significant harm to a consumer seeking a loan.

Recent studies by the Consumer Federation of America have documented a huge variation in the credit scores reported by different repositories, and a significant number of errors that could affect as many as two-fifths of consumers. (See "The Credit Score Lottery" on page 21.)

By giving consumers better access to their credit reports and notification of negative information that has been furnished to a credit bureau, some states have facilitated an important safety check in the current systematic collection of consumer data.

The cost to consumers of inadequate safeguards for private financial information

In the wake of technological advances that have outpaced consumer safeguards, big banks and financial service companies are fighting to maintain a system in which consumers bear the burden of protecting their good name, peace of mind, and most personal information. Meanwhile, these financial service companies reap the profits of exploiting private information. Last year, these profits amounted to $937 million in California alone, according to an analysis by the Direct Marketing Association.[52]

These industry profits, however, do not come without a price—a price that currently, consumers are forced to pay.

Taking away consumer privacy, then selling it back
Increasingly, financial companies have developed customer services to respond to the concerns of consumers—at a price. For example, a customer calling to check up on whether their credit statement reflects a recent transaction will be told, "You're clearly very responsible and concerned about the security of your credit, Ms. X. Would you like to purchase special credit protections at only $50 annually?"

Although common practices in the financial services industry often make it more difficult to adequately prevent and prosecute identity theft, many of these same corporations benefit from the problem by marketing products and services to prevent identity theft or mitigate its effects.

Equifax offers a service called "Credit Watch™ Gold" for over $100/year, and Experian offers a similar service called "Credit Manager" for $80/year.

A survey conducted by Privacy and American Business found that one in six consumers reported buying a privacy protection product to help avoid identity theft, to check their credit report, or to surf or shop online anonymously, at an average annual price of $75. Extrapolating these figures to one in six consumers nationwide (34 million Americans), Privacy and American Business concluded that this represents a $2.5 billion market for privacy products.

The growing retail market for privacy protections demonstrates that privacy conscious consumers, in the absence of strong consumer safeguards, are increasingly forced to "foot the bill" for safeguards sold back to them by the same financial companies who share and sell their information.

The price consumers pay

A comprehensive analysis of costs that could reasonably be attributed to current inadequacies of information safeguards should include the burden placed on consumers by identity theft crimes, the time required to "opt-out" of information sharing (if current problems with readability and understandability of privacy notices were solved), and the costs of privacy protection products and services that consumers are increasingly resorting to in the absence of strong legal standards.

Table 1. Out-of-Pocket Costs to Consumers Resulting From Inadequate Privacy Safeguards

	Out-of-Pocket Cost to Consumers	# Of People Affected Annually
ID Theft	$5 billion[53]	10 million
Privacy Protections	$2.5 billion[54]	1 in 6 households (17.8 million)
Total	$7.5 billion	

As Tables 1 and 2 show, the financial impact to consumers of having inadequate privacy safeguards in direct out-of-pocket expenses ($7.5 billion) plus the costs in lost time (1.06 billion hours, translating to $11.2 billion) is significant, even without assigning a monetary value to pain, suffering, and frustration caused by privacy violations.

These numbers demonstrate that economically, lack of adequate information safeguards can be assigned a cost to consumers of at least $18.7 billion, or $175 per household. This cost ignores costs of identity theft to businesses (estimated at $50 billion annually) and lost Internet sales (estimated at $18 billion annually), which arguably trickle down to consumers—for example, when interest rates increase as a result of losses from companies who write off goods and services that were stolen by identity thieves.[55]

Members of the financial services industry have argued elsewhere that consumers derive benefits from the sale and sharing of their private information. These benefits, they argue, result from relationship pricing, proactive offers, targeted marketing, and third party services.

Even if the strongest privacy bills under consideration in state legislatures become law, consumers who value these potential benefits more highly than the costs and inconvenience of abridged privacy will have the ability to "opt-in," thus allowing their personal information to be shared with businesses in order to attain these benefits—regardless of what types of privacy protections are in place.

Table 2. CALPIRG Analysis of Costs to Consumers In Time Spent Due to Inadequate Privacy Safeguards

	Time Spent	Number of People Impacted	Aggregate Time	Monetary value of time
ID Theft[56]	30 hours each victim	10 million	300 million hours	$4.6 billion
Privacy Protections	10 minutes to purchase,	17.8 million	3 million hours	$46 million
Opt-out[57]	5 hrs per household	84.3 million	420 million hours	$6.5 billion
Total	6.8 hours		723 million hours	$11.2 billion

However, consumers who value their privacy over these potential benefits should have similar power to limit the sharing of their personal information.

Opting out takes time and money

The average household receives between thirty and fifty privacy notices every year. For example, one columnist described the types of notices he received over the course of one summer season: (W. Scott Blackmer)

Thus, I have notices from General Motors (for my car lease), Sears (for a home improvements account), the company administering my pension plan, Sallie Mae (for the student loan I co-signed), the issuers of each credit card in my wallet and my wife's, the mortgage company, the office and computer supply store where I have a store card, each bank where I have any kind of account (including those for kids away at college), and the companies behind every life, auto, homeowner's, disability, and travel insurance policy that we own. It adds up. According to industry estimates, most established households in America have received about 20 notices this season.[58]

Many privacy notices may never be noticed. However, for the privacy conscious consumer, reading and responding to such notices each year may require a significant investment of time.

Industry studies estimate "Costs of Consumer Privacy"

The financial services industry has attempted to frame the financial privacy policy debates around a single issue—the hypothesized monetary benefits of information sharing—that ignores the real damages consumers are suffering from loss of control over their personal information. Several industry reports have estimated financial benefits that companies derive from current lax privacy practices, in some cases extending these estimates of benefits to consumers.

One study, conducted for the Financial Services Roundtable, involves an analysis of subjective estimates of how consumers would be impacted if "nonpublic financial information" could not be shared with affiliates and sold to third parties. This study, which is based on opinions of executives at 48 of the largest financial service companies in the nation (and all of them members of the group that funded the study), estimated that households served by those companies could pay a premium of $195 and 4 hours lost time if sharing of "nonpublic financial information" were limited.[59]

Such studies should be interpreted with caution. For example, this particular study is:

- funded by companies that profit from selling and sharing private information;
- based not on verifiable data but rather on estimates of industry executives; and
- methodologically flawed in that it is only representative of the largest financial conglomerates, and not of the community and state institutions that continue to serve millions of Americans. In fact, many community banks do not perform direct marketing outside their own customer base and continue to use traditional underwriting tools, rather than relying solely on automated underwriting.[60] Such institutions are likely to be impacted less significantly than the large national conglomerates surveyed in this study. However, the study assumes in effect that all customer relationships nationwide are with Roundtable members.

This study includes further flaws in methodology likely to lead to an overestimation of the benefits derived from information sharing.[61] It can hardly be taken as a thorough analysis of burdens that may be placed on consumers when a corporation protects their privacy.

Privacy and profitability can go hand in hand

Not all financial services companies profit from the absence of consumer privacy protections. Many consumers will forego purchasing products from retailers when they are not confident of the ultimate use of their information. For example, members of the financial services industry who rely on the Internet for much of their operations may benefit significantly from stronger privacy protections, benefits they could then pass on to consumers. One analysis estimated that companies doing business over the Net could lose up to $18 billion in annual sales because of privacy concerns.[62]

Some national financial services institutions are leading the way in acknowledging consumers' right to privacy, and leading the industry economically as well. For example, E-Loan has been more aggressive in empowering consumers' right to financial privacy. This institution, which reported record revenues in the second quarter of 2003 and played an active role in winning passage of California's recent financial privacy legislation, gives consumers the right to opt in for information sharing with third parties:

> *We do not sell or share your information with third party marketers. So, there is no need for you to ask us not to. In fact, there is no need for you to opt-out of any information sharing because, unlike most financial*

> *institutions, we provide you with an opt-in. This means we won't share your information unless you explicitly tell us to, even though the law allows financial institutions to share your information unless and until you tell them not to. Additionally, although the law allows financial institutions to share your information with other financial institutions under a "joint marketing agreement" without your consent, we don't.*

In addition, countless community banks relying on personal relationships with customers have never sold or shared customer information. Chittenden Bank, for example, operates in Vermont, New Hampshire, Massachusetts, and Maine, and has simply made a corporate decision to not share customer information in any of the ways that customers would be able to opt-out of under federal law.[63]

Community and state banks are less likely than their national counterparts to perform direct marketing outside their own customer base and less likely to depend solely on credit reports for their lending decisions. An independent survey of 146 financial institutions (half of the respondents were state-chartered banks) found that only 25% of financial institutions answering this question share customer data with third party marketing firms, and less than one-third reported sharing data with a parent company or holding company.[64]

Conclusion

In the wake of rising identity theft and information sharing abuses, Americans are understandably concerned about the misuse of personal information. In the absence of strong state protections, companies may benefit from the collection and sale of consumers' most personal information, leaving individuals to bear the costs in money, frustration, and time spent to assert their own privacy rights.

Legislatures in 21 states have passed policies to help in some degree restore the balance between fair information principles that protect consumers' private information and the drive of free enterprises to profit from this information. Consumers in the states with the strongest protections benefit from better credit rates than the national average, while enjoying the same benefits of the information economy as residents in less privacy-oriented states.

Much progress must still be made to ensure that all Americans have control of their most personal information. Under the current system, a small but continuously growing percentage of the population is subject to substantial harm from abuse of their personal information. A wide segment of the privacy-sensitive population must overcome significant hurdles to exercise any control over the sharing of their information with third parties. And no one, outside the states of California, Vermont, and Alaska, has the ability to restrict how banks share information with affiliated institutions.

State governments have served as financial privacy policy incubators. In doing so, they have allowed consumers to express their priorities in creatively rebalancing the scales that tend to tip toward industry profit and away from consumer protection.

State laws that have resulted in gains for consumers should serve as the foundation to establish stronger privacy protections nationwide, ensuring all Americans are governed by policies that enact the Fair Information Principles. The state governments have proved more adept at finding ways to give consumers access to the information that is collected on them, assurance that the information is accurate, control over how the records are used and by whom, and the ability to easily overcome problems that result from abuse.

Endnotes

[1] Privacy and American Business/Louis Harris & Associates, *Privacy Concerns and Consumer Choice Survey*, December 1998.
[2] Ibid.
[3] For example, raising health insurance premiums for someone whose credit card statements reveal purchases from a company that sells rock climbing gear. For a hypothetical but plausible story of the ways that this can be abused, see Minnesota Attorney General Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests In The 21st Century*, 2001.
[4] Rickie Windle, "NationsSecurities losses hit home: Local investor one of seven named litigants in Texas lawsuit against NationsBank subsidiary," *Austin Business Journal*, 26 May 1995.
[5] Anuradha Raghunathan, "Predatory lending document could target CitiFinancial," *Knight Ridder/Tribune News Service*, 13 September 2002.
[6] Minnesota Attorney General Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests In The 21st Century*, 2001.
[7] The Attorney General of the State of New York, Bureau of Consumer Frauds and Protection, "In the matter of Chase Manhattan Bank USA, N.A." January 2000. Available at www.oag.state.ny.us/internet/litigation/chase.pdf.
[8] Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, 22 January 2003, 8.
[9] Federal Trade Commission, *Identity Theft Survey Report*, September 2003, 4.
[10] Ibid., 7.
[11] Janine Benner, California Public Interest Research Group/Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft*, May 2000.
[12] Identity Theft Resource Center, *Identity Theft: The Aftermath 2003*, September 2003.
[13] See note 9, 43-46.
[14] See note 9, 47.
[15] See note 12.
[16] See note 9, 33.
[17] See note 9, 29.
[18] See note 9, 39.
[19] Mary Allen, "Former First USA Bank employee pleads guilty to identity theft" *The News Journal* (Wilmington, DE), 7 February 2003.
[20] Brooke A. Masters, "Mass Theft of Identities Alleged; 30,000 victimized; U.S. Charges Computer Worker," *Washington Post*, 26 November 2002.
[21] Benjamin Weiser, "Identity ring said to victimize 30,000," *New York Times*, 26 November 2002.
[22] Steven Church and Sean O'Sullivan, "Identity thieves get inside help," *The News Journal* (Wilmington, DE), 28 July 2002.
[23] Steven Church, "3rd person guilty of credit fraud," *The News Journal* (Wilmington, DE), 13 May 2000.
[24] Consumer Federation of California, *Financial Privacy Initiative Press Conference* (press release), 12 March 2003.
[25] Harris Interactive, *Most People Are "Privacy Pragmatists" Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits*, March 2003.
[26] Ibid.
[27] Harris Interactive, *Privacy On and Off the Internet: What Consumers Want*, February 2002.
[28] See note 25.
[29] See note 25.
[30] See note 25.
[31] See note 27.
[32] Jedediah Purdy, "An intimate invasion," *USA Weekend*, 2 July 2002.
[33] E-LOAN, *Study Finds California Voters Want Stronger Financial Privacy Protection Laws*, 21 February 2002.
[34] Edmund Mierzwinski, USPIRG Consumer Program Director, "Recommendations to Improve the Fair Credit Reporting Act," Testimony Before the US Senate Banking Committee, 31 July 2003.

[35] Adapted from the Organization for Economic Cooperation and Development's *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 1980.
[36] More information on the FACT Act can be obtained at http://www.pirg.org/consumer/pdfs/fcrafinalsumm.pdf.
[37] See, for example, Michael E. Staten and Fred H. Cate, Credit Research Center, *The Impact of National Credit Reporting Under the Fair Credit Reporting Act: The Risk of New Restrictions and State Regulation*, May 2003.
[38] Most of the following restrictions on information sharing have certain exceptions. For example, personal information may frequently be disclosed when responding to a court subpoena, completing a transaction requested by the consumer, or detecting fraud. Also, many statutes vary somewhat in the sort of information that is covered. See each statute for specifics.
[39] Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, July 2001.
[40] Steve Blackledge, CALPIRG, *Privacy Denied: A Survey of Bank Privacy Policies*, August 2002.
[41] Bryan O'Malley and E. Joyce Gould, *Your Privacy is Important to Us?,* October 2001.
[42] Leland Chan and James Clark, "Financial Information Privacy Act Would Breed Copycat Problems," *American Banker*, 5 October 2001.
[43] Association of Bay Area Governments, *Consumer Financial Privacy: Local Government Ordinances and Resources*, downloaded from <www.abag.ca.gov/privacy>, 23 October 2003.
[44] Robert B. Avery, Paul S. Calem, and Glenn B. Canner, Federal Reserve Board's Division of Research and Statistics, "An Overview of Consumer Data and Credit Reporting," February 2003.
[45] Consumer Federation of America, *Credit Score Accuracy and Implications for Consumers*, 17 December 2002. The data was gathered and the analysis done with no personally identifying information, ensuring that no records could be tied to actual individuals.
[46] Ibid., 38.
[47] Ibid., 5.
[48] This follows the work of Fordham University Professor Joel Reidenberg (see his 8 May 2003 testimony before the House Subcommittee on Financial Institutions and Consumer Credit, financialservices.house.gov/media/pdf/050803jr.pdf) and Vermont Assistant Attorney General Julie Brill (see her 4 June 2003 testimony before the Subcommittee on Financial Institutions and Consumer Credit, financialservices.house.gov/media/pdf/060403jb.pdf). We have expanded this analysis from the three states that had laws exempted from the 1996 FCRA preemption (Vermont, California, Massachusetts), and instead average over these and all the states that have restricted information-sharing in a way that industry studies suggest would be unacceptable. Also, we have gone back several more years, to do five-year averages.
[49] It is possible but very difficult to verify that rather than raise mortgage rates lenders might restrict access to credit by changing the consumer credit score eligible for prime rates. This raises another problem with the current system: consumers have little access to the criteria (in terms of numerical scores) used to assign prime rates for credit. In effect, credit is calculated in a black box using algorithms developed by the firm of Fair, Isaac—algorithms to which consumers do not have access. A good treatment of this issue can be found on the web at <www.fool.com/specials/2000/sp000807.htm>.
[50] Federal Housing Finance Board, *Monthly Interest Rate Survey: Periodic Summary Tables*, downloaded from www.fhfb.gov/mirs/mirs_downloads.htm, 27 October 2003.
[51] Data on non-business bankruptcy filings per year in each state: American Bankruptcy Institute, *Bankruptcy Filings by State*, downloaded from www.abiworld.org/stats/bystate.html, 10 October 2003. Number of households per state available from the U.S. Census Bureau at www.census.gov.
[52] Jane Black, "Privacy: For Every Attack, a Defense," *Business Week,* 22 July 2003.
[53] See note 9.
[54] Privacy and American Business press release presenting Harris Interactive polling results downloaded October 15, 2003 at www.pandab.org/privacyproducts_pr.html.
[55] Sandeep Junnarkar, "Report: Half of Net users mistrust sites," *CNET News.com*, 17 August 1999.
[56] See note 9.
[57] Our estimate is based on the following assumption:
80% of households would read notices if they were understandable, each household receiving 30 privacy notices annually, 10 minutes required to read each notice, average hourly wage $15.45 (US Labor

Department, as cited by Joseph Rebello and Phil McCarty , "Unemployment Rate Holds at 6.1% in September," Dow Jones Newswires, 3 October 2003). These do not reflect actual percentages of people reading or responding to these notices under the current system, in which privacy notices are frequently overlooked and unintelligible, but in a system based on consumers' reported preferences.

[58] W. Scott Blackmer, "Financial Privacy Notices: Worth Noticing," downloaded from http://www.juniper.com/app/ccsite/legal/overviewDynamic.jsp, 27 October 2003.

[59] Ernst and Young, *Customer Benefits from Current Information Sharing by Financial Services Companies*, conducted for the Financial Services Roundtable, December 2000.

[60] Bill Stoneman, "Lenders Paint Bleak Picture Of Post-Preemption World," *American Banker,* 11 June 2003.

[61] A full discussion of these methodological flaws would treat the conflation of a company's revenues with number of customers, which introduces significant error, as well as the assumption that each customer has all financial relationships within the 100 Roundtable companies, none with outside companies. An error analysis of simply one source of error in the industry study, in which revenue is used as a proxy for number of customers although their correlation is 0.8, reveals a margin of error of $3-4 billion.

[62] Sandeep Junnarkar, "Report: Half of Net users mistrust sites," *CNET News.com*, 17 August 1999.

[63] Gordon Raymond, Vice President and Director of Compliance for Chittenden Corporation, personal communication, 8 September 2003.

[64] Walter Kitchenman, "2002 Best Privacy Practices Survey," submitted as public comment to the Federal Trade Commission as part of a workshop, "Get Noticed: Effective Financial Privacy Notices," 4 December 2001.

U.S. Public Interest Research Group

Consumer Federation of America

Consumers Union
Publisher of Consumer Reports

2003 Changes to the Fair Credit Reporting Act: Important Steps Forward at a High Cost

With passage of HR 2622, the Fair and Accurate Credit Transactions Act, Congress significantly amended the Fair Credit Reporting Act (15 USC 1681 *et seq.*), which provides consumer protections regarding the use, accuracy and privacy of consumer credit reports. This law, originally passed in 1970, ensures that consumers have access to information about them that lenders, insurers, and others obtain from credit bureaus and use to make decisions about providing credit and other services. Amendments passed in 1996 provided new consumer rights to improve accuracy of reports, but in exchange for these increased consumer rights, states were temporarily preempted from passing stronger protections in a few specific areas of the law. Those preemptions were scheduled to expire on January 1, 2004, which thrust this important law into the spotlight in 2003 as industry lobbyists sought to make those preemptions permanent.

The changes to the Fair Credit Reporting Act passed by Congress this year make some improvements for consumers to increase the accuracy of credit reports, prevent identity theft, and restrict the marketing of financial products using sensitive information that is shared with affiliates. In addition the FCRA amendments provide for one free credit report per year from each agency and guarantee consumers access to credit scores at a reasonable fee. However, these improvements come at the very high price of permanent preemption of state action in the areas preempted since 1996, as well as expansion of preemption to include several new areas addressed in this year's legislation. In addition, many of the new consumer protections provided in the 2003 amendments solely rely on agency enforcement and explicitly do not allow consumers a federal private right of action to sue violators.

Except where specifically indicated, these changes will be effective within one year of enactment. The Federal Reserve Board and the Federal Trade Commission (FTC) have two months to issue regulations establishing effective dates for each section, which should occur as early as possible, but no later than ten months after the issuance of these regulations or no later than 365 days following the signing of Public Law 108-159 on 4 December 2003.

The following is a summary prepared by Consumer Federation of America, Consumers Union and U.S. PIRG of the principal changes made to the FCRA by enactment of the FACT Act.

ID Theft

Prior to enactment of the FACT Act, Congress had only enacted one law in response to the growing crime of identity theft. In 1998, Congress made identity theft a felony and ordered the FTC to coordinate federal efforts to monitor the crime. The FACT Act makes several changes to the FCRA, largely based on already-enacted state laws.

One Call Fraud Alerts: Establishes the right of any consumer to request a fraud alert for 90 days or, if a consumer provides an "identity theft report" (which could include an FTC ID theft affidavit if filed with a law enforcement agency), the consumer could place an extended fraud alert of seven years in his or her credit file. The alert must be included with a credit report and with the delivery of a credit score. Users of reports and scores have a new duty to honor fraud alerts. They cannot issue a new credit line, extension of credit, new cards or a requested higher credit limit on existing accounts unless the consumer is called or other reasonable verification steps are taken. Any national credit bureau contacted by a consumer must inform other bureaus that a fraud alert has been placed (one-call fraud alert). Non-national bureaus are required to advise consumers how to contact national bureaus. Persons who file an extended fraud alert are automatically opted out of pre-screening for five years. Active duty military personnel gain the right to request one-year "active-duty" alerts. All consumers who place an alert may receive a free credit report. Persons who place an extended fraud alert may also get two free reports in the first year.

Trade Line Blocking: Requires Consumer Reporting Agencies (CRAs, or credit bureaus) to block fraudulent trade lines when a consumer provides an identity theft report, provided that it has been filed with a law enforcement agency.

Business Records Disclosure: Allows ID theft victims with a police report (a higher standard than "identity theft report") to request and get copies of records from businesses where a thief opened accounts or obtained goods or services, to help clear their names. The business may insist on a police report, and may take 30 days to provide the information.

Red Flag Guidelines for New Accounts and Change of Address Verification: Regulators are required to establish guidelines for issuers to follow to identify patterns and practices leading to identity theft. The regulations will require reasonable procedures to comply with the guidelines. The regulations will also require card issuers to verify changes of address in certain circumstances (e.g. when a request for a new card comes within 30 days following a change of address).

Credit Card Number Truncation On Consumer Reports: Requires credit card machines to truncate all credit and debit card numbers on non-manual receipts by 2007.

Social Security Number Truncation: Allows a consumer to request that the credit report disclosed to the consumer truncate any included Social Security Numbers.

Prohibits Sale or Collection of ID Theft Debts: Prohibits any person or business from selling, transferring, or placing for collection any item subject to an identity theft trade line block or debt which resulted from identity theft once the block has been placed and the creditor has notice of

the block. (However, there is an exemption for information provided in the securitization of debts)

Debt Collector Notice Requirements: Any third party debt collector that is notified that the debt they are trying to collect may be fraudulent must notify the third party and also must provide the consumer upon request with notice of his or her rights in debt collection.

Prevention of Repollution: Creditors and others who furnish information to a CRA and who are notified by a CRA of the existence of an identity theft trade line block must maintain reasonable procedures to prevent refurnishing (repollution) of the information arising from the ID theft. A furnisher receiving an identity theft report at a proper address may not refurnish such information unless it subsequently verifies that information.

Accuracy, Access to Reports and Reinvestigations

Studies have shown that credit reports and resulting credit scores are often inaccurate or incomplete, resulting in consumers paying too much for credit. Further, consumers face difficulty fixing mistakes. (The major provision of the 1996 amendments was the imposition, for the first time, of duties on companies providing information to credit bureaus, known as furnishers.) The following FACT Act amendments address accuracy, access and reinvestigations.

Annual Free Credit Reports: Each national credit bureau must provide a free report upon request within 15 days of a request by phone, Internet, or mail through a one-call centralized source to be established by the FTC within a year. Reports will also be available from specialty bureaus, such as landlord – tenant or insurance reporting services, with the method of distribution to be established in regulations to be issued within six months, effective six to nine months thereafter. States are preempted from increasing the frequency of the provision of free reports (free report laws in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Vermont are "grandfathered").

Reinvestigations: CRAs have 45 days to conduct reinvestigations of disputed items resulting from free report requests (compared to 30-45 days for all other reinvestigations). This does not apply if the CRA has not been continuously providing consumer reports for 12 months preceding request.

FTC To Create Summary Of Rights For Consumers: These rights include the availability of free credit reports, the right to dispute information in a credit report, and how to request and obtain credit score. The summary of rights will be distributed with adverse action notices (if a consumer is denied or offered credit at less than favorable terms) and actively promoted by FTC and posted on its website. This summary must also tell consumers that they may have additional rights under state law.

Credit Bureaus Must Provide Credit Scores, and information on up to four key factors (or five factors if the number of inquiries was a factor and not among the four key factors) adversely affecting a consumer's score. Bureaus can charge a "fair and reasonable fee" for score, as determined by the FTC. This does not apply to mortgage scores, such as those created by automated underwriting programs.

Mortgage Lenders Must Provide Credit Scores, and information on key factors lowering a consumer's score to those who apply for mortgages. No fee is authorized for this disclosure. States are preempted from acting further regarding the disclosures of credit scores for credit granting purposes (California and Colorado statutes grandfathered). States are allowed to continue to act in the area of insurance scores, credit based scores used in connection with insurance, and credit score issues other than disclosure issues.

One-Time Written Notification That Negative Information Will Be Or Has Been Sent To Credit Bureaus: Any financial institution that submits negative information to national CRA must give consumers one-time written notice that they have done so or will do so. This notice may be included in a notice of default or a billing statement, but not with Truth in Lending disclosures.

New Risk Based Pricing Notice: Existing law provides that consumers who are denied credit or services or required to pay extra for credit due to their credit report receive an "adverse action notice" triggering their credit reporting rights. The FACT Act establishes a new notice for certain additional circumstances. Whenever credit is extended on terms "materially less favorable than the most favorable terms available to a substantial proportion of consumers" from that creditor, creditors must provide notice that the terms offered are based on information in a consumer's credit report and that the consumer can request a free copy of the report. (No civil enforcement is allowed -- federal enforcement only. States are preempted from acting further with respect to the notice.)

Guidelines/Regulations On Accuracy And Integrity Of Information: The FTC and financial regulators are to create guidelines for accuracy and integrity of information and require furnishers of information to establish reasonable policies and procedures to implement guidelines.

Higher Standard For Furnishers Of Information To CRAs: Under pre-revision rules, those who provide information to credit reporting agencies were not allowed to report inaccurate information if they knew or consciously avoided knowing that the information was inaccurate. The new standard prohibits reporting of inaccurate information if the furnisher "knows or has reasonable cause to believe that the information is inaccurate."

Consumers Can Dispute Incorrect Information Directly With Furnisher: Under pre-revision rules, furnishers of information were only required to perform a reinvestigation of the accuracy of information if they received a complaint from a consumer *via a credit reporting agency*. The new law requires financial regulators and the FTC to prescribe regulations outlining circumstances when creditors and other furnishers of information to CRAs should reinvestigate complaints that come directly from a consumer. (Exempts disputes filed by credit repair organizations. This new right does not provide a private right of action .)

FTC Compilation And Report On Complaints Regarding Credit Reports: CRAs must report on the determinations made based on such complaints. Requires the FTC to compile an annual report on the outcome of these complaints.

Study Of Accuracy And Completeness Of Consumer Reports: The Federal Reserve Board and FTC must study and report to Congress (twelve months after enactment) on the compliance of

CRAs and furnishers regarding the accuracy of items by consumers, the completeness of information provided to CRAs, and the correction and deletion of inaccurate or incomplete information.

Improved Disclosure Of Results Of Reinvestigation: CRAs must notify furnishers when changes are made because of a reinvestigation based on a consumer complaint about a credit reporting error.

Requirement For Furnishers To Update Records: Furnishers must change records, delete records, or permanently block reporting to CRAs of information found to be inaccurate or incomplete.

Notification Of Address Discrepancy: CRAs must notify anyone requesting a consumer's report if the address on the request substantially differs from the address in the consumer's file.

Reasonable Reinvestigation: Clarifies the obligation on CRAs to reinvestigate items of disputed accuracy by requiring a "reasonable reinvestigation".

FTC Study And Report on Credit Reporting Issues: The FTC must submit a report within one year on ways to improve operation of the FCRA, including:

- Whether requiring requesters of credit reports to match more points of identifying information before a report is issued would increase accuracy and reduce ID theft;
- The impact of notifying consumers when negative information is added to a report on consumers' ability to identify errors on credit reports and to remove fraudulent information from reports;
- The impact of requiring that consumers who suffer an adverse action based on a credit report immediately receive a copy of the credit report used for the decision on consumers' ability to identify errors and remove fraudulent information;
- The impact of including non-traditional transaction information on determining consumers creditworthiness, and how to encourage voluntary reporting of such information, and
- A study on the use of biometrics and other technologies to fight ID theft.

Ongoing FTC Study Of And Reports On The Accuracy And Completeness Of Consumer Reports: An Interim report is due in one year, and biennially thereafter for eight years. The final report is due two years after that.

Privacy

The FCRA also requires that users of credit reports have a "permissible purpose" to obtain them, mandates that CRAs maintain the security and integrity of consumer files, and allows consumers to limit certain uses of their reports.

Stronger Opt-Out For Prescreening Based On Credit Report Information: Prescreened offers of credit must contain a phone number to opt out of such offers in a simple and easy to understand format, as outlined by regulation within one year of enactment. Extends the duration of the telephone-initiated opt out from two years to five years. (Under current law, a mailed "notice of

election" results in a permanent opt out.) FTC must take measures to increase awareness of the opt out number, and study the opt out process, including current mechanisms available for consumers to opt out, the extent to which consumers are utilizing these measures, the benefits and costs to consumers of receiving prescreened offers of credit or insurance, the impact of further restricting written offers on cost, availability, and consumer knowledge of new products, on competition, and on reaching underserved populations (report due within one year).

New Opt-Out For Marketing Solicitations That Are Based On Information Shared Among Affiliates: Consumers must be provided the opportunity to opt out of receiving solicitations for marketing purposes based on information shared among corporate affiliates, effective for at least five years, after which the consumer must be given notice and the opportunity to opt out again. Exempts marketing when a preexisting relationship has existed with customers within 18 months, for employee benefit plans, and to perform services on behalf of an affiliate (but one affiliate cannot solicit on behalf of an affiliate that is prohibited from soliciting), and in response to communications initiated by the consumer or in response to solicitations initiated by or requested by consumer. Does not apply to information received prior to the effective date of regulations. This notice can be combined with other notices. (Regulations will be issued within nine months; effective six months after issuance).

Study Of Information Sharing: Requires federal financial services agencies and the FTC to study the following: the purposes for which affiliate sharing information is used; the types of information shared with affiliates; choices provided to consumers regarding control of sharing and the degree to which consumers use options; if information is used for employment or hiring, or for general publication of such information; and the information sharing practices that financial institutions and other creditors and users of consumer reports employ for purposes of credit underwriting or evaluation. (Report due within three years, and required every three years thereafter in identifying changes in use of information and reduced need for credit reports as a result.)

Disposal Of Consumer Information And Records Containing Consumer Information: Final regulations due within one year, and will address methods of disposal but not require the destruction of records.

Medical Information Protections: Any medical information in a consumer report must be coded to obscure the specific healthcare provider and the nature of medical services provided. Creditors are prohibited from obtaining or using medical information in credit decisions. (Final regulations for limitation on creditors due within six months, effective 90 days thereafter.) Prohibits the sharing among affiliates of medical information, including individual or aggregate lists based on payments for products or services. (The remainder of the medical privacy section is effective 180 days after enactment.) Medical providers must identify themselves as such within 15 months.

Other Important Provisions

Statute of Limitations: Amended to overturn Supreme Court decision in *Andrews vs. TRW* and provide for opportunity to sue two years following discovery or five years following date of violation, whichever is earlier.

Credit Score Study: Requires the FTC, the Federal Reserve Board and HUD to study and report on (within two years) the effects of the use of credit scores and credit-based insurance scores on the availability and affordability of financial products and services for all Americans, and for various minority groups, as well as any negative or differential treatment of protected classes under the Equal Credit Opportunity Act.

Financial Literacy Improvement: Establishes a Financial Literacy Education Commission made up of representatives of various federal agencies, to be led by the Secretary of Treasury. The Commission is charged with developing a national strategy to promote financial literacy and education (within 18 months) and with disseminating financial literacy information. As part of the national strategy, the Treasury Department is allocated three million dollars to conduct a national public service multimedia campaign to improve financial literacy in 2004, 2005 and 2006. The Comptroller General must conduct a study (within three years) of the effectiveness of the Commission's efforts and on how to improve financial literacy among consumers.

Workplace Investigations: The FACT Act weakens certain protections provided to employees when investigations are conducted in the workplace of alleged sexual harassment, embezzlement, drug use, etc.

State Preemptions

The original 1970 FCRA provided that the law would provide minimum federal protections that the states could exceed. The 1996 amendments provided that states would be preempted from enacting stronger laws in seven particular provisions of the FCRA, but only until 1 January 2004, unless Congress acted to renew the preemptions.

1) The FACT Act makes permanent the seven preemptions enacted in 1996 and otherwise set to expire. These cover:

- Prescreening of consumer reports;
- The time frames for handling accuracy disputes;
- The duties of persons who take adverse actions (notices and disclosures);
- The duties of persons who use consumer reports in connection with credit or insurance transactions not initiated by a consumer;
- Information contained in consumer reports;
- The duties of furnishers of information to consumer reporting agencies, and
- The sharing information among affiliates (although the interplay between this provision and other federal laws, such as the Gramm-Leach-Bliley Act, authorizing state action has not been determined).

2) The FACT Act enacts the following new preemptions. These cover:

- The obligation on businesses who grant credit or provide goods or services to ID thieves to provide information to victims;
- Consumers' rights to opt out of solicitations based on affiliate shared information ;
- Risk based pricing notices;

- Annual free credit reports (with grandfathering of existing laws), and
- Credit score disclosure by CRAs and by mortgage lenders when the score is for credit granting purposes;

3) The FACT Act enacts narrower ID theft preemptions, whereby state laws are restricted only with respect to the "conduct required by the specific provisions of" these identified sections of the FCRA:

- The truncation of credit or debit card numbers on receipts;
- The placement of fraud alerts and active duty military alerts;
- The blocking of information resulting from ID theft;
- Allowing consumer to request truncation of Social Security Numbers on communications sent to them;
- Red flag guidelines regarding ID theft;
- Prohibiting the sale or collection of debts resulting from ID theft and requiring third party debt collectors to notify creditors if they learn that a debt has resulted from ID theft;
- The referral process between CRAs regarding ID theft complaints, fraud alerts, and blocking of information;
- Various disclosures, including the summary of rights to obtain credit report and score and to dispute information, the summary of ID theft victim rights, and the right of ID theft victim to get information from businesses;
- Procedures to prevent refurnishing of information resulting from ID theft;
- Annual free credit reports for ID theft victims (this is listed in two parts of the bill), and
- The disposal of records containing information from credit reports.