Testimony of Edmund Mierzwinski
Consumer Program Director
U.S. Public Interest Research Group (U.S. PIRG)

On behalf of
Consumer Action
Consumer Federation of America
Consumer Task Force on Automotive Issues and Remar Sutton, President
Consumers Union
Electronic Privacy Information Center
Identity Theft Resource Center
Junkbusters, Inc
Privacy Rights Clearinghouse
Private Citizen, Inc.
U.S. PIRG

Oversight Hearing On Financial Privacy and the Gramm-Leach-Bliley Financial Services Modernization Act

Committee on Banking, Housing and Urban Affairs
United States Senate

The Honorable Paul Sarbanes, Chairman

19 September 2002

Chairman Sarbanes and Members of the Committee, thank you for the opportunity to testify before you today. As you know, U.S. PIRG[1] serves as the national lobbying office for state Public Interest Research Groups, which are independent, non-profit, non-partisan research and advocacy groups with members around the country. Our testimony is also on behalf of Consumer Action, Consumer Federation of America, Consumer Task Force on Automotive Issues and Remar Sutton, President, Consumers Union, Electronic Privacy Information Center, Identity Theft Resource Center, Junkbusters, Inc, Privacy Rights Clearinghouse, Private Citizen, Inc.[2] Many of these groups participating are members of the Privacy Coalition.[3]

SUMMARY

Congress knew that the 1999 Gramm-Leach Bliley Financial Services Modernization Act[4] (GLBA) – a law long-sought by the financial industry to encourage the creation of integrated financial services firms -- would exacerbate already-identified financial privacy threats. So Congress incorporated Title V to protect financial privacy, which included the following five key provisions. The most important and most successful is the last: the fail-safe states' rights provision allowing states to enact stronger financial privacy laws.

(1) Title V defined certain confidential information as "non-public personal information" subject to strong privacy protection.

Status: An important recent decision by the DC Circuit US Court of Appeals upholding the GLBA financial privacy regulations has effectively closed the so-called credit header loophole exploited by Internet information brokers to obtain Social Security Numbers from credit bureaus without consumer consent. Creating a strict definition of protected information is an important and successful result of GLBA.

(2) Title V required covered firms to provide, by July 2001, annual notice of their information sharing practices with both affiliated and non-affiliated third parties.

Status: The core of the GLBA privacy scheme is limited to notice. Industry lobbyists will falsely portray their distribution of billions of privacy notices as successful privacy protection. Notice is not enough to protect privacy. Data collectors should adhere to a broader set of Fair Information Practices (discussed below). Worse, the first year's privacy notices were unreadable; this year's no better. Although notice is not enough to protect privacy, covered firms should do a better job of providing notice and regulators should penalize those that do not.

(3) Title V required covered firms to provide in that notice an extremely limited statutory consumer right to opt-out (affirmatively act to say no) to the sharing of information with some, but not all, non-affiliated third parties. Transactions between affiliates and also with many non-affiliated third parties engaged in joint marketing contracts with an affiliate could continue regardless of whether or not a customer had chosen to "opt-out."

Status: Notice is not enough, nor is the limited opt-out, to satisfy the Fair Information Practices. The vast majority of all information sharing with both affiliates and many third parties is only covering by notice, not by this limited opt-out "right." The provision is inadequate and fails to even rein in the practices of the telemarketers it is narrowly targeted at (see (4) below). The partial opt-out should be replaced by an across-the-board affirmative consent (opt-in) provision for all affiliate and third party information sharing. The failure of the GLBA to require any form of consumer consent for the vast majority of information sharing transactions affected is one example of how GLBA fails to meet the Fair Information Practices (discussed below).

(4) Title V attempted, through an encryption provision, to restrict the tawdry practice of non-affiliated telemarketers obtaining credit card numbers from banks, then signing consumers up for expensive "membership clubs" and billing them when the consumer failed to affirmatively cancel within 30 days.

Status: As Attorneys General Hatch of Minnesota and Sorrell of Vermont have testified today, telemarketers continue to find loopholes enabling them to bill consumers for products the consumer never ordered, using credit card numbers provided by the consumer's bank, **not** by the consumer. Consumers don't think they ordered anything, when they don't hand over cash, a check or a credit card number. Unfortunately, the encryption provision has codified, instead of stopped, the growing epidemic of anti-consumer, controversial "pre-acquired account telemarketing."

(5) Finally, recognizing that it hadn't really completed the job of protecting privacy adequately, the Congress– in an extremely rare departure from its normal policy of preempting state action -- explicitly included a fail-safe provision allowing states to enforce existing and enact new stronger financial privacy laws.

Status: The states' rights fail-safe is the most important, and most successful, privacy protection in GLBA. We commend the Chairman for his sponsorship of the provision added in conference committee known as the "Sarbanes amendment." States have been very active and although not all have yet been successful, we believe that there is a good chance that passage of strong new privacy laws in a few more states will provide Congress with the encouragement it needs to raise the bar nationally.

FINANCIAL PRIVACY AND THE GRAMM-LEACH-BLILEY ACT

The 1999 Gramm-Leach-Bliley Financial Services Modernization Act was enacted to respond to changes in the marketplace. Banks, insurance companies and securities firms were more and more selling products that looked alike. The firms wanted the privilege of and synergies derived from selling them all under one roof. Yet, the Gramm-Leach-Bliley Act was also enacted against a backdrop of financial privacy invasions, and members wanted to ensure that the new law wouldn't make things worse. Consumer and privacy groups argued that if the Congress was going to create one-stop financial supermarkets, then privacy protections ought to extend to all information sharing, whether with affiliates or with third parties. At the time, two examples were given of the need for stronger privacy laws.

- First, Nationsbank (now Bank of America) had recently paid civil penalties totaling $7 million to the Securities and Exchange Commission and other agencies, plus millions more in private class action settlements, over its sharing of confidential bank accountholder information with an affiliated securities firm. "Registered representatives also received other NationsBank customer information, such as financial statements and account balances."[5] In this case, conservative investors who held maturing certificates of deposits (CDs) were switched into risky financial derivative products. Some lost large parts of their life savings.
- Second, Minnesota Attorney General Mike Hatch had recently sued US Bank and its holding company, accusing them of having "sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for $4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks."[6] As General Hatch has testified today in detail, Memberworks and other non-affiliated third party telemarketers sign credit card customers up for add-on "membership club" products and bill their credit cards as much

as $89 or more if they do not cancel within 30 days. The catch? The consumer never gave the telemarketer her credit card number; her bank did, in a scheme known as pre-acquired account telemarketing. General Hatch has settled with both US Bank and Memberworks.

Industry has argued that these "aberrations" occurred before the enactment of GLBA. Yet, as General Hatch has also testified today, however, he has also recently settled a post-GLBA lawsuit with Fleet Mortgage Company over similar practices in the post-GLBA environment[7]. He and numerous other Attorneys General have filed comments with the US Treasury Department and the Federal Trade Commission seeking stronger laws restricting "pre-acquired account telemarketing" transactions involving banks and membership clubs run by telemarketers.

In response to these documented concerns about the risks to financial privacy, Congress included a specific financial privacy title in the Gramm-Leach-Bliley Act.

Basic Structure of the GLBA Financial Privacy Scheme and Its Limitations

The principal privacy protection in GLBA is an annual notice requirement. GLBA defines non-public personal information that must be protected. GLBA then requires covered entities to disclose their information sharing policies with both affiliated companies (companies under the same corporate umbrella and "common control") and with non-affiliated third parties. GLBA then requires firms to grant customers a limited right to opt-out of a small number of transactions with some non-affiliated third parties (primarily telemarketers).

The opt-out applies to neither affiliates nor any non-affiliated third parties in a joint marketing relationship with the bank or other covered entity. The rationale for treating marketing partners as affiliates was ostensibly to create a level playing field for smaller institutions that might not have in-house affiliates selling every possible product larger firms might sell.[8] Of course, large firms use joint marketing partners, too.

The result of this scheme is that most information-sharing is only "protected" by notice. Sharing of confidential consumer information with either affiliates or joint marketing partners continues regardless of a consumer's privacy preference. Although we have no way of knowing how many joint marketing partners a company may have, we do know how many affiliates some of the largest financial services holding companies and bank holding companies have. For their recent joint comments to the Treasury Department on GLBA, state Attorneys General accessed the Federal Financial Institutions Examination Council and Federal Reserve websites and counted affiliates for Citibank (2,761), Key Bank (871) and Bank of America (1,476).[9]

The GLBA has failed to provide adequate protections for consumer privacy in modern financial services. Individuals face a multitude of potential risks through unrestricted and undisclosed information-sharing of personal financial data information under the GLBA. Unfettered affiliate and non-affiliate sharing permits comprehensive profiling, which results in aggressive target marketing techniques, identity theft, profiling and fraud. Consumers have not been adequately informed or been given effective choice to evaluate the benefits of information-sharing against the potential harms causes by unrestricted information-sharing.

The inherent weaknesses of GLBA notwithstanding, the July 2002 decision by the Court of Appeals upholding GLBA's regulations is nevertheless an important decision upholding the constitutionality of a broad government privacy regulation.[10] Government has an important interest in protecting privacy and regulating the activities of companies that share and sell confidential consumer information. Financial privacy is not merely an issue of a few "nuisance"

phone calls, as industry would like to portray it. When data collectors do not adhere to Fair Information Practices (discussed below) consumers face numerous privacy risks:

- Consumers pay a much higher price than dinner interruptions from telemarketers. Many unsuspecting constituents of yours may be paying $89/year or more for essentially worthless membership club products they did not want and did not order.
- Easy access to confidential consumer identifying information leads to identity theft. Identity theft may affect 500-700,000 consumers each year. Identity theft victims in a recent PIRG/Privacy Rights Clearinghouse survey faced average out-of-pocket costs of $808 and average lost time of 175 hours over a period of 1-4 years clearing an average $17,000 of fraudulent credit off their credit reports. It is difficult to measure the costs of higher credit these consumers pay, let alone attempt to quantify the emotional trauma caused by the stigma of having their good names ruined by a thief who was aided and abetted by their bank and credit bureau's sloppy information practices[11].
- Reliance on the Social Security Number as a unique identifier in the private sector has proliferated. Easy access to Social Security Numbers by Internet information brokers and others also leads to stalking.
- The failure to safeguard information and maintain its accuracy leads to mistakes in credit reports and consequently consumers pay higher costs for credit or are even denied opportunities.
- Although industry witnesses will testify to a vast "free flow of information" driving our economy that should not be constrained, more and more firms are choosing to stifle the flow of information themselves -- to maintain their current customers as captive customers. When a bank intentionally fails to report a consumer's complete credit report information to a credit bureau, that consumer is unable to shop around for the best prices and other sellers are unable to market better prices to that consumer.[12]
- The unlimited collection and sharing of personal data poses profiling threats. Profiles can be used to determine the amount one pays for financial services and products obtained from within the "financial supermarket" structure. As just one example, information about health condition or lifestyle can be used to determine interest rates for a credit card or mortgage. Even with a history of spotless credit, an individual, profiled on undisclosed factors, can end up paying too much for a financial service or product. Because there are no limits on the sharing of personal data among corporate affiliates, a customer profile can be developed by a financial affiliate of the company and sold or shared with an affiliate that does not fall within the broad definition of "financial institution." A bank, for instance, that has an affiliation with a travel company could share a customer profile resulting in the bank's customer receiving unwanted telephone calls and unsolicited direct mail for offers of memberships in travel clubs or the like that the individual never wanted or requested[13].

We will now discuss the success or failure of the five key privacy provisions summarized above in greater detail.

(1) Title V defined certain confidential information as "non-public personal information" subject to strong privacy protection.

Status: An important recent decision by the DC Circuit, US Court of Appeals upholding the GLBA financial privacy regulations has effectively closed the so-called credit header loophole exploited by Internet information brokers to obtain Social Security Numbers from credit bureaus without consumer consent. Creating a strict definition of protected information is an important and successful result of GLBA.

The GLBA created a category of protected "non-public personal information." The final GLBA financial privacy rules issued by 7 federal financial agencies defined Social Security Numbers as non-public personal information (NPPI). A key provision is that the transfer of Social Security Numbers from financial institutions to credit bureaus is **only** allowed for regulated Fair Credit Reporting Act purposes (eg, for use in a credit report) but not for unregulated purposes, where the credit bureau would be considered a non-affiliated third party. The agencies correctly interpreted the law to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out.

In 1993, the Federal Trade Commission had (improperly in our view) granted an exemption to the definition of credit report when it modified a consent decree with TRW (now Experian). The FTC said that certain information would not be regulated under the Fair Credit Reporting Act (FCRA). The so-called credit header loophole allowed credit bureaus to separate a consumer's so-called header or identifying information from the balance of an otherwise strictly regulated credit report and sell it to anyone for any purpose. Credit headers included information ostensibly not bearing on creditworthiness and therefore not part of the information collected or sold as a consumer credit report. The sale of credit headers involves stripping a consumer's name, address, Social Security Number and date of birth[14] from the remainder of his credit report and selling it outside of the FCRA's consumer protections. Although the information, marketing and locater industries contend that header information is derived from numerous other sources, in reality, the primary source of credit header data is likely financial institution information.

In their unsuccessful arguments to the courts, the credit bureau Trans Union and a number of companies that sell information, organized into the now-apparently-defunct Individual References Services Group, argued that GLBA included a Fair Credit Reporting Act savings clause and therefore their sale of Social Security Numbers was legal. As the FTC explains in the preamble to its Gramm-Leach-Bliley Financial Privacy Rule:

> The Commission recognizes that § 313.15(a)(5) permits the continuation of the traditional consumer reporting business, whereby financial institutions report information about their consumers to the consumer reporting agencies and the consumer reporting agencies, in turn, disclose that information in the form of consumer reports to those who have a permissible purpose to obtain them. Despite a contrary position expressed by some commenters, this exception does not allow consumer reporting agencies to re-disclose the nonpublic personal information it receives from financial institutions other than in the form of a consumer report. Therefore, the exception does not operate to allow the disclosure of credit header information to individual reference services, direct marketers, or any other party that does not have a permissible purpose to obtain that information as part of a consumer report. Disclosure by a consumer reporting agency of the nonpublic personal information it receives from a financial institution pursuant to the exception, other than in the form of a consumer report, is governed by the limitations on reuse and redisclosure in § 313.11, discussed above in "Limits on reuse." Those limitations do not permit consumer reporting agencies to disclose credit header information that they received from financial institutions to nonaffiliated third parties. … If consumer reporting

> agencies receive credit header information from financial institutions outside of an exception, the limitations on reuse and re-disclosure may allow them to continue to sell that information. This could occur if the originating financial institutions disclose in their privacy policies that they share consumers' nonpublic personal information with consumer reporting agencies, and provide consumers with the opportunity to opt out. [Emphasis added, Footnotes omitted][15]

There is a slight chance that credit bureaus will eventually convince financial institutions to provide notice of their sharing of Social Security Numbers, triggering the right to share Social Security Numbers for consumers who do not opt-out. So, Congress should act to close the credit header loophole completely. Several House bills and a Senate bill, S. 1014, sponsored by Senator Bunning of the Banking Committee (although the bill has been referred to the Finance Committee) would completely close the credit header loophole and take other steps to improve Social Security Number privacy.

In the 106th Congress, legislation named for the first-known victim of an Internet stalker was defeated after it was seen that the proposal actually was a Trojan Horse that expanded the availability of Social Security Numbers to customers of the Individual References Services Group (IRSG). IRSG member companies included credit companies and other information firms engaged in the sale of non-public personal information to information brokers, private detectives and others.[16] The IRSG was established as a supposed self-regulatory organization and received a tacit endorsement from the Federal Trade Commission[17] for its efforts to police its industry. The association reportedly has dissolved following its unsuccessful attempts to overturn the GLBA regulations.

(2) Title V required covered firms to provide, by July 2001, annual notice of their information sharing practices with both affiliated and non-affiliated third parties.

Status: The core of the GLBA privacy scheme is limited to notice. Industry lobbyists will falsely portray their distribution of billions of privacy notices as successful privacy protection. Notice is not enough to protect privacy. Data collectors should adhere to a broader set of Fair Information Practices (discussed below). Worse, the first year's privacy notices were unreadable; this year's no better. Although notice is not enough to protect privacy, covered firms should do a better job of providing notice and regulators should penalize those that do not.

The notices provided by banks, securities firms and other covered institutions have been widely panned by a variety of experts for their inscrutable, dense language. While the banks and others have complained that the law required such detail, we respectfully disagree that the law required banks to confuse customers. Mark Hochhauser, readability consultant to the Privacy Rights Clearinghouse, analyzed dozens of the initial notices: "Readability analyses of 60 financial privacy notices found that they are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public.[18]"

In response, a number of consumer and privacy groups formed a coalition to petition the financial regulatory agencies to strengthen the notices using existing authority. Apparently in response to the petition of 26 July 2001 and other complaints, the agencies held a workshop in December 2001. We are unaware of significant improvement to the notices in 2002. According to the petition filed by the consortium of consumer and privacy groups:

> In passing §§ 501-510 of the GLBA, Congress gave consumers the right to prevent financial institutions from transferring their personal financial information to third parties. To that end, the Act requires the institutions to notify customers of the right to opt

> out and to provide convenient means of exercising it. However, in notices mailed out thus far, most financial institutions have employed dense, misleading statements and confusing, cumbersome procedures to prevent consumers from opting out. Such notices evince a clear failure of the Act's implementing regulations to effectuate congressional intent. Accordingly, we ask the Agencies to revise the regulations and require that financial institutions provide understandable notices and convenient opt-out mechanisms.[19]

According to a smaller August 2002 California PIRG survey [20]of 10 bank privacy notices issued in the second year, 2002: "Most banks receive a failing grade and the best received a "C-."

As for the notion that no company would seek to make notices confusing on purpose, so consumers would fail to take advantage of an opt-out right, we would encourage the committee to review a recent federal court decision. The U.S. district court decision in the case *Darcy Ting et al vs. AT&T* describes how the long-distance carrier AT&T may have used consultants to help it write legal notices to its customers in such a way that the consumers would view an amendment to their customer service agreement (CSA) as a "non-event" and not either "opt-out" of the change or, worse, "defect" to another carrier. The key provision reduced legal remedies (by requiring mandatory arbitration). From the district court ruling:

> 22. AT&T conducted market research to assist it in developing the contract documents. One part of AT&T's research, the Quantitative Study, included the following key findings and recommendations:
>
> > In the letter it should be made clear that this agreement is being sent for informational purposes only. The fact that no action is required on the part of the customer needs to be made. (sic) …
>
> 23. Another part of AT&T's research, the Qualitative Study, concluded that after reading the bolded text in the cover letter which states "**[p]lease be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to do**," "[a]t this point most would stop reading and discard the letter." (emphasis in original)…
>
> … 24. … While presenting the CSA as a non-event may have helped AT&T retain its customers, it also made customers less alert to the fact that they were being asked to give up important legal rights and remedies.
>
> (US District court decision, *Darcy Ting et al vs. AT&T*[21]*)*

(3) Title V required covered firms to provide in that notice an extremely limited statutory consumer right to opt-out (affirmatively act to say no) to the sharing of information with some, but not all, non-affiliated third parties. Transactions between affiliates and also with many non-affiliated third parties engaged in joint marketing contracts with an affiliate could continue regardless of whether or not a customer had chosen to "opt-out."

Status: Notice is not enough, nor is the limited opt-out, to satisfy the Fair Information Practices. The vast majority of all information sharing with both affiliates and many third parties is only covering by notice, not by this limited opt-out "right." The provision is inadequate and fails to even rein in the practices of the telemarketers it is narrowly targeted at (see (4) below). The partial opt-out should be replaced by an across-the-board affirmative consent (opt-in) provision for all affiliate and third party information sharing.

The failure of the GLBA to require any form of consumer consent for the vast majority of information sharing transactions affected is one example of how GLBA fails to meet the Fair Information Practices.

Ideally, consumer groups believe that all privacy legislation enacted by either the states or Congress should be based on Fair Information Practices, which were originally proposed by a Health, Education and Welfare (HEW) task force and then embodied into the 1974 Privacy Act and into the 1980 Organization for Economic Cooperation and Development (OECD) guidelines. The 1974 Privacy Act applies to government uses of information.[22] Consumer and privacy groups generally view the following as among the key elements of Fair Information Practices:

1) Collection Limitation Principle: 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 Principle: 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 Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4) Use Limitation Principle: 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 Principle: 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 Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) Individual Participation Principle: 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 Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.[23]

Consumer groups disagree with industry organizations over whether certain self-regulatory or statutory schemes are adequately based on Fair Information Practices. Industry groups often seek to block legislation or offer substitute legislation intended to "dumb-down" the Fair Information Practices, as they were able to do with GLBA.

- First, industry groups seek to substitute a weaker opt-out choice, instead of providing opt-in consent before secondary uses,
- Second, industry groups claim that notice is enough. They claim that right of review and correction are unnecessary.
- Third, they contend that either agency enforcement or self-regulation is an adequate substitute for a consumer private right of action (also missing from GLBA).

Privacy advocates and other consumer groups believe that consumers should provide consent for all information sharing circumstances—by and among both affiliates and third parties. Second, that protection should be on an opt-in basis since it gives consumers control.

How The Gramm-Leach-Bliley Act Falls Short of the Fair Information Practices:

First, it fails to require any form of consent (either opt-in or opt-out) for most forms of information sharing for secondary purposes, including experience and transaction information shared between and among either affiliates or affiliated third parties.

Second, while consumers generally have access to and dispute rights over their account statements, they have no knowledge of, let alone rights to review or dispute, the development of detailed profiles on them created by financial institutions.

The act does provide for disclosure of privacy policies, although a review of a sample of privacy policies suggests that companies are not following the spirit of GLBA. See (3) above. None are fully explaining all their uses of information, including the development of consumer profiles for marketing purposes. None are listing all the types of affiliates that they might share information with. None are describing the specific products, most of which are of minimal or even negative value to consumers, that third party telemarketers might offer for sale to consumers who fail to opt-out. Yet all the privacy policies make a point of describing how consumers who elect to opt-out will give up "beneficial" opportunities.

(4) Title V attempted, through an encryption provision, to restrict the tawdry practice of non-affiliated telemarketers obtaining credit card numbers from banks, then signing consumers up for expensive "membership clubs" and billing them when the consumer failed to affirmatively cancel within 30 days.

Status: As Attorneys General Hatch of Minnesota and Sorrell of Vermont have testified today, telemarketers continue to find loopholes enabling them to bill consumers for products the consumer never ordered, using credit card numbers provided by the consumer's bank, not by the consumer. Consumers don't think they ordered anything, when they don't hand over cash, a check or a credit card number. Unfortunately, the encryption provision has codified, instead of stopped, the growing epidemic of anti-consumer, controversial "pre-acquired account telemarketing."

In December 2000, the Minnesota Attorney General filed a new suit against Fleet Mortgage, an affiliate of FleetBoston, for substantially the same types of violations as U.S. Bank engaged in. That complaint was settled in June. The state's complaint explains the problem with sharing

confidential account information with third party telemarketers. The complaint states that when companies obtain a credit card number in advance, consumers lose control over the deal:

> Other than a cash purchase, providing a signed instrument or a credit card account number is a readily recognizable means for a consumer to signal assent to a telemarketing deal. Pre-acquired account telemarketing removes these short-hand methods for the consumer to control when he or she has agreed to a purchase. The telemarketer with a pre-acquired account turns this process on its head. Fleet not only provides its telemarketing partners with the ability to charge the Fleet customer's mortgage account, but Fleet allows the telemarketing partner to decide whether the consumer actually consented. For many consumers, withholding their credit card account number or signature from the telemarketer is their ultimate defense against unwanted charges from telemarketing calls. Fleet's sales practices remove this defense.[24]

This complaint alleged that the company was providing account numbers to the telemarketer. In our view, either Gramm-Leach-Bliley or the FTC Telemarketing Sales Rule needs to be amended so that telemarketers cannot initiate the billing of a consumer who has not affirmatively provided his or her credit card or other account number. Whether this case stems from pre-Gramm-Leach-Bliley acquisition of full account numbers, or post-Gramm-Leach-Bliley encrypted numbers or authorization codes, is not the question. In either case, consumers have lost control over their accounts.

How do the credit card companies and telemarketers respond to consumer complaints? Data from consumer complaints to U.S. PIRG and to the FTC and the legal complaints and accompanying materials of the State of Minnesota all show the following pattern: Consumers who call their credit card company to complain about their bills are transferred to the telemarketer, whose agents were trained to continue to try to confuse the consumer. The telemarketer then claims that the consumer assented to the confusing trial offer by giving their "date of birth" or some other piece of information (but not of course a credit card number, let alone an "expiration date."). Sometimes the telemarketer would play a piece of recorded tape from the call where the consumer had provided a date of birth—arguing that providing your date of birth was proof that the consumer had agreed to the transaction. This response to complaints made about unauthorized charges was designed to convince consumers to "eat" the charge.

Providing a date of birth in response to a trick question is not providing a credit card number to order a product. Pre-acquired account telemarketing should be banned. We are encouraged that the proposed FTC amendments to the Telemarketing Sales Rule would ban pre-acquired account telemarketing.[25]

No bank – indeed, no firm – should be allowed to earn commissions from companies (whether affiliated, joint marketing partners, or third party telemarketers) that bill consumers for products they do not want and have not ordered, through the scheme known as "pre-acquired account telemarketing," which eliminates a consumer's fundamental control over her purchase decisions by allowing the consumer's bank to make purchase decisions for her and bill her credit card without her knowledge or consent.

(5) Finally, recognizing that it hadn't really completed the job of protecting privacy adequately, the Congress– in an extremely rare departure from its normal policy of preempting state action -- explicitly included a fail-safe provision allowing states to enforce existing and enact new stronger financial privacy laws.

Status: The states' rights fail-safe is the most important, and most successful, privacy protection in GLBA. We commend the Chairman for his sponsorship of the provision added in conference committee known as the "Sarbanes amendment." States have been very active and although not all have yet been successful, we believe that there is a good chance that passage of strong new privacy laws in a few more states will provide Congress with the encouragement it needs to raise the bar nationally.

Our organizations and others, including, as state representative Jim Kasper reports today, the grassroots-based Protect Our Privacy coalition in North Dakota, have fought to enact stronger privacy protections in state law. While we have faced significant opposition from vested financial interests, we strongly believe that the fail-safe states' rights' provision of Title V is its most important provision.

Five states have some form of 'opt-in' financial privacy provisions: Alaska, Connecticut, Illinois, Maryland, and Vermont. Each has laws applying to different aspects of financial information. In three states, legislative repeals of stronger pre-GLBA legislation occurred in 2000-2001: North Dakota, Maine and Florida. However, in June 2002, North Dakota citizens reversed that state's repeal action on a 73%-27% ballot referendum vote. [26] The result of the referendum was reinstatement of the previous opt-in based law.

Vermont is the only state that has a law that specifically regulates affiliate sharing.[27] The state of Vermont is also vigorously defending a lawsuit by insurance associations seeking to overturn its financial privacy laws.

Consumers Union, Privacy Rights Clearinghouse, California PIRG and other groups have been strong supporters of proposed California legislation by State Senator Jackie Speier. As originally introduced, SB 773[28] would have required that all information sharing, whether by and between affiliates or with third parties, would require opt-in consent. In its final form, although still defeated in the state assembly last month, the bill would have required an opt-out for all sharing between either affiliates or non-affiliated joint marketing partners (no consent protection under federal law) and required an opt-in for sharing with other third parties (opt-out under current federal law).

Passage of SB 773, even in its weakened form, would have granted California consumers vastly improved financial privacy rights over current law.

In our view, passage of such a strong bill in such a large state would have had a very good chance to lead to similar federal legislation, vindicating the fail-safe states' rights model adopted by GLBA. The success of the citizens of North Dakota and the near success of the California legislature in enacting the Speier bill, despite an overwhelming campaign by the industry, strongly suggest that the states' rights provision of Title V has been successful and should be continued.

We are also encouraged that extant preemption provisions in the Fair Credit Reporting Act (15 USC 1681 *et seq.*) expire on 1 January 2004. At that time, states will be free to experiment with strengthening both of the core laws protecting their financial privacy—FCRA and GLBA. Uncertainty over the relationship between the FCRA's preemption provisions and GLBA's FCRA savings clause regarding affiliate sharing has helped the financial industry to successfully oppose state laws seeking to further regulate financial privacy. When that FCRA preemption provision expires, there will be greater clarity for legislators about states' rights to regulate affiliated transactions.

RECOMMENDATIONS

(1) STRENGTHEN GLBA

The Gramm-Leach-Bliley Act should be strengthened. Consumers should be granted an affirmative informed consent right (opt-in) before non-public personal information is shared with either affiliates or third parties.

Providing informed consent and providing notice are only two of a set of Fair Information Practices that give consumers control over the use of their confidential information. Protection of privacy requires data collectors to adhere to all of the Fair Information Practices. Efforts by industry groups to "dumb-down" the Fair Information Practices should be resisted.

(2) RESIST EFFORTS TO ELIMINATE STATES' RIGHT TO ENACT STRONGER LAWS

Congress should resist efforts by industry lobbies to eliminate the right of states to pass stronger financial privacy laws. Congress should also reject proposed federal legislation (HR 3068) and similar amendments to place a moratorium on stronger financial privacy laws.

In addition, Congress should reject the specious claims of some financial industry lobbyists that strong state privacy laws deter homeland security. According to a February 2002 Associated Press story:

> The banking industry is reaching out to Homeland Security Director Tom Ridge and lawmakers in search of federal help to block state consumer privacy laws that bankers argue will hinder their efforts to spot terrorists. Industry lobbyists have been arguing that state laws that prohibit banks from sharing consumer information without permission might preclude them from alerting law enforcement to potential crimes. "We would have trouble communicating with law enforcement ... and it would be extremely chaotic. We need a uniform privacy standard," said David Liddle of the Financial Services Roundtable, an industry lobby. …"[29]

As far as we know, Director Ridge has not dignified these requests with any comment.

(3) REJECT CLAIMS THAT COSTS OF PRIVACY ARE TOO HIGH

We urge the Congress to reject industry claims that privacy's costs are too high and its benefits too low. We have reviewed a number of presumably-industry-funded studies purporting to make this claim and find their methodology lacking. We refer the committee to an alternate study, by an independent consultant, which critiques the industry studies and points out numerous benefits of privacy as well as the **costs of <u>insufficient</u> privacy protection**. As Robert Gellman points out:

> The cost of privacy is a legitimate issue, but the studies and the conclusions drawn from them have serious flaws… **In fact, the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year.** [Emphasis added.] [30]

CONCLUSION:

Thank you for the opportunity to provide our views before the committee today on the important matter of financial privacy. You, Mr. Chairman, and other committee members, especially Senator Shelby and Senator Dodd, Senate Co-Chairs of the Bi-Partisan Congressional Privacy Caucus, should be commended for your leadership on financial privacy. We look forward to working with you to strengthen consumer privacy rights.

ENDNOTES

[1] U.S. PIRG (www.uspirg.org) is the national lobbying office for the State Public Interest Research Groups (www.pirg.org). State PIRGs are non-profit, non-partisan public interest advocacy groups.
[2] Consumer Action, (www.consumer-action.org) founded in 1971, is active on privacy issues both in California and on the national level working through its network of more than 6,500 community based organizations. Consumer Federation of America (www.consumerfed.org) is a coalition of 240 national, state and local consumer groups around the country. Consumer Advocate Remar Sutton is President of the Consumer Task Force on Automotive Issues (http://www.autoissues.org/). He and the Task Force are founding members of www.privacyrightsnow.com Consumers Union (www.consumer.org) is the non-profit, non-partisan, non-commercial publisher of Consumers Reports magazine and maintains advocacy offices in California, Washington, DC and Texas. The Electronic Privacy Information Center (EPIC) (www.epic.org) was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. The Identity Theft Resource Center (http://www.idtheftcenter.org/) is a nationwide nonprofit organization dedicated to developing and implementing a comprehensive program against identity theft. Junkbusters, Inc. (www.junkbusters.com) offers free software and other tools to fight junk mail, spam, cookies, and other forms of privacy invasion. The Privacy Rights Clearinghouse (www.privacyrights.org) is a nonprofit consumer information and advocacy program. Private Citizen, Inc (http://www.private-citizen.com/) is nationally known and respected as America's foremost consumer organization fighting against the direct marketing industry's privacy-abusive practices.
[3] The Privacy Coalition was established in 2001 by a broad range of consumer, privacy, civil liberties, family-based and conservative organizations that share strong views about the right to privacy. The groups had previously worked together on a more informal basis in opposition to the intrusive Know-Your-Customer rules and in support of financial privacy proposals offered in the 106th Congress by members of the bi-partisan Congressional Privacy Caucus, co-chaired by Senate Banking Committee members Richard Shelby and Christopher Dodd and House Energy and Commerce Committee members Joe Barton and Ed Markey. Groups endorsing the coalition's legislative candidate Privacy Pledge are listed at the website PrivacyPledge.Org.
[4] Public Law 106-102, 15 U.S.C. § 6801, et seq. enacted November 12, 1999
[5] See the SEC's Nationbank Consent Order <http://www.sec.gov/litigation/admin/337532.txt>
[6] See the complaint filed by the State of Minnesota against US Bank <http://www.ag.state.mn.us/consumer/privacy/pr/pr%5Fusbank%5F06091999.html>
[7] See the complaint filed by the State of Minnesota against Fleet Mortgage, 28 December 2000, http://www.ag.state.mn.us/consumer/news/pr/Comp_Fleet_122800.html
[8] The GLBA also includes numerous other exceptions to opt-out protections, including sharing for government or law enforcement purposes and sharing for purposes related to completing a consumer transaction (such as a credit card purchase or ATM withdrawal).
[9] See 1 May 2002 Attorneys General Comments http://www.ots.treas.gov/docs/r.cfm?95421.pdf or <http://www.epic.org/privacy/financial/ag_glb_comments.html> on the GLBA Information Sharing Study (Federal Register: February 15, 2002 (Volume 67, Number 32))
[10] See http://pacer.cadc.uscourts.gov/common/opinions/200207/01-5202a.txt
[11] See "Nowhere To Turn: A Survey of Identity Theft Victims, May 2000,CALPIRG and Privacy Rights Clearinghouse, <http://calpirg.org/CA.asp?id2=3683&id3=CA&>
[12] See speech by Comptroller of the Currency John Hawke at http://www.occ.treas.gov/ftp/release/99-51.txt 7 June1999: "Some lenders appear to have stopped reporting information about subprime borrowers to protect against their best customers being picked off by competitors. Many of those borrowers were lured into high-rate loans as a way to repair credit histories." According to U.S. PIRG's sources in the lending industry, this practice continues.
[13] For additional discussion of the profiling issue, and related privacy threats posed by information sharing, see 1 May 2002 comments of EPIC, US PIRG, Consumers Union, and Privacy Rights Clearinghouse on the GLBA Information Sharing Study (Federal Register: February 15, 2002 (Volume 67, Number 32)) available at <http://www.epic.org/privacy/financial/glb_comments.pdf>
[14] In a separate 2001 decision by the DC Circuit, US Court of Appeals (No. 00-1141, 13 April 2001, *cert denied*, 10 June 2002 by Supreme Court), *Trans Union I vs. FTC*, <http://laws.findlaw.com/dc/001141a.html> the FTC's order against Trans Union <http://www.ftc.gov/os/2000/03/transunionopinionofthecommission.pdf> prohibiting Trans Union from selling actual credit information for illegal marketing purposes was upheld. This decision also

removed dates of birth from credit headers, since age is a determinant of credit scores and therefore has a bearing on creditworthiness. See

[15] Excerpted from pages 80-83, Federal Trade Commission, 16 CFR Part 313, Privacy Of Consumer Financial Information, Final Rule <http://www.ftc.gov/os/2000/05/glb000512.pdf>

[16] See the U.S. PIRG Fact Sheet, "Why The Amy Boyer Law Is A Trojan Horse" at <http://www.pirg.org/consumer/trojanhorseboyer.pdf>

[17] See for example, Testimony of FTC Commissioner Mozelle Thompson before the House Banking Committee, 28 July 1998, http://www.ftc.gov/os/1998/9807/pretexttes.htm.

[18] See "Lost in the Fine Print: Readability of Financial Privacy Notices" by Mark Hochhauser at http://www.privacyrights.org/ar/GLB-Reading.htm

[19] The petition is available at http://www.privacyrightsnow.com/glbpetition.pdf . See the website http://www.privacyrightsnow.com for additional information about the coalition.

[20] See the CALPIRG report Privacy Denied: A Survey Of Bank Privacy Policies, 15 Aug 2002, <http://calpirg.org/CA.asp?id2=7606&id3=CA&>

[21] See especially paragraphs 21-24 of US District Judge Bernard Zimmerman's 15 January 2002 opinion in *Darcy Ting et al vs AT&T* (Case 01-02969BZ, Northern District of California). Now on appeal to the 9th Circuit Court of Appeals.

[22] As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html> The document cites the version of FIPs in the original HEW guidelines, as well as other versions.

[23] Organization for Economic Cooperation and Development, *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980), at <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM> as quoted in Gellman, "Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete," March 2002, http://www.epic.org/reports/dmfprivacy.html or <http://www.cdt.org/publications/dmfprivacy.pdf>.

[24] 28 December 2000, Complaint of State of Minnesota vs. Fleet Mortgage, see <http://www.ag.state.mn.us/consumer/news/pr/Comp_Fleet_122800.html>

[25] See 67 FR 4492 available at http://www.ftc.gov/os/2002/01/16cfr310.pdf

[26] See the website of the North Dakota grassroots group that beat the banks 73%-27% in a June referendum on financial privacy at http://www.protectourprivacy.net/

[27] Comments of 44 Attorneys General to Federal Trade Commission Regarding GLB Notices. February 15, 2002 (available at www.naag.org).

[28] See legislative history of SB 773 at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_773&sess=CUR&house=B&author=speier

[29] See "Banks Seek to Block State Privacy Laws," 19 February 2002, Sharon Thiemer, Associated Press.

[30] See Gellman, "Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete", March 2002, http://www.epic.org/reports/dmfprivacy.html or <http://www.cdt.org/publications/dmfprivacy.pdf>.