

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

**Hearing On
“An Examination of Existing Federal Statutes Addressing Information Privacy”**

**Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce**

The Honorable Cliff Stearns, Chairman

3 April 2001

Chairman Stearns, Representative Towns and Members of the Committee, thank you for the opportunity to testify before you today. As you know, U.S. PIRG 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.

U.S. PIRG is also a founding member of the Privacy Coalition, established this year 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 Congressional Privacy Caucus, co-chaired by 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.

The emphasis of my testimony today is on the two major laws affecting financial privacy—the 1999 Gramm-Leach-Bliley Financial Services Modernization Act [Public Law 106-102, 15 U.S.C. § 6801, et seq. enacted November 12, 1999 and its interrelationship with the 1970 Fair Credit Reporting Act [Public Law No. 91-508, 15 U.S.C. § 1681 et seq. (October 26, 1970)]. We concur with the testimony today of Consumers Union on information privacy issues more broadly.

SUMMARY

The 1970 Fair Credit Reporting Act (FCRA), its major 1996 amendments, and Title V, Privacy, of the Gramm-Leach-Bliley (GLB) Act were all enacted in response to privacy nightmares. Unfortunately, the 1996 FCRA amendments included an affiliate-sharing exception to the definition of credit report, allowing companies to share confidential consumer information subject to very few consumer protections. This meant the Congress had to consider privacy issues related to affiliate-sharing when it enacted GLB.

Although GLB does not go as far as consumer and privacy groups wanted, it should not be weakened. The federal financial regulatory agencies correctly interpreted statutory intent when they included Social Security Numbers in the definition of Non-Public Personal Information under the act. The lawsuit seeking to overturn the rule, filed by several firms that sell credit headers (previously unregulated locator products that include Social Security Numbers obtained from financial institution customers) should be dismissed. In addition, the federal financial regulatory agencies correctly defined the term “financial institutions” broadly to encompass all firms engaged in financial activities.

The Gramm-Leach-Bliley Act should be strengthened by extending and expanding its current opt-out choice provision. Consumers should be granted an opt-in consent right before non-public personal information is shared with either affiliates or third parties.

Providing informed consent is one of a set of Fair Information Practices that give consumers control over the use of their confidential information. Efforts by industry groups to “dumb-down” the Fair Information Practices should be resisted. Notice is not enough.

BACKGROUND

The basic structure of information privacy law is to place responsibilities on organizations that collect personal data and to give rights to individuals that give up their data. This is sensible for many reasons, including the fact that it is the entity in possession of the data that controls its subsequent use. Information privacy law also promotes transparency by making data practices more open to scrutiny and encourages the development of innovative technical approaches.¹

Privacy laws, particularly in the United States, are widespread and have invariably come about in response to new technologies and new commercial practices. From the telephone, to the computer database, to cable television, electronic mail, videotape rentals, and the Internet, the American tradition is to establish a right of privacy in law to enable the development of new commercial services.

While it is true that the U.S. has recently relied on a sector-by-sector approach to privacy, rather than an over-arching privacy law, the convergence of industry sectors that is occurring has accelerated the need for consideration of an over-arching privacy law, which would protect consumers both online and offline in all transactions. An example of this convergence is the changes in the financial marketplace that necessitated enactment of the Gramm-Leach-Bliley Act. As privacy expert Marc Rotenberg has noted, it is now time to consider such an over-arching privacy law:

Those who argue that the United States has typically protected privacy by self-regulation and industry codes know very little about the long tradition of privacy legislation in this country. It is, however, correct to say that the United States, over the last twenty years, has taken a sectoral approach as opposed to an omnibus approach to privacy protection in the private sector. But it is also important to note that the sectoral approach has several weaknesses. For example, we have federal privacy laws for video records but not for medical records. There are federal privacy laws for cable subscriber records but not for insurance records. I think the problems with the sectoral approach will become increasingly apparent as commerce on the Internet grows. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. For the vast majority of transactions, simple, predictable uniform rules offer enormous benefits to consumers and businesses. It is also becoming increasingly clear that the large industry mergers in the telecommunications and financial services sectors have made the sectoral approach increasingly obsolete. Firms now obtain information about individuals from many different sources. There is a clear need to update and move beyond the sectoral approach.²

THE CODE OF 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. That act applies to government uses of information.³ Consumer and privacy groups generally view the following as among the key elements of Fair Information Practices:

- limitation to collection of necessary information (purpose specificity),
- notice of the existence of all databases to data subjects who are then granted a concomitant right of disclosure of their record to review, dispute and correct errors,
- a restriction on secondary uses without consumer consent,
- a guarantee that data collectors maintain the accuracy and security of databases,
- no preemption of state or local laws affording greater protection,
- and, a private right of action for data subjects if the other rights have been violated.

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:

- 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 disclosure and correction rights are unnecessary.
- Third, they support preemption of stronger state laws and also contend that either agency enforcement or self-regulation is an adequate substitute for a consumer private right of action.

HISTORY OF CONSIDERATION OF FAIR CREDIT REPORTING ACT AND GRAMM-LEACH-BLILEY PRIVACY PROVISIONS

(1) The Need For a Fair Credit Reporting Act

U.S. PIRG has long been interested in financial information privacy issues. In 1989, we first testified before the Congress on the need for amendments to the 1970 Fair Credit Reporting Act (FCRA). At that time, in a series of hearings, Congress noted a shocking rise in the number of complaints about credit report inaccuracies to state attorneys general and the Federal Trade Commission.

The 1970 act had been enacted in response to two major problems. First, consumers had no control over the use or accuracy of their factual credit reports (called “consumer reports” in the statute). Second, job, credit and insurance applicants had been victimized by abusive collection of information, by credit bureaus, for the preparation of “investigative consumer reports.” An investigative consumer report is a credit report that is based on subjective and hearsay interviews with neighbors and co-workers.⁴

In 1991, we published the first of a series of PIRG reports on the accuracy and privacy of consumer credit reports. To date, we have published six reports on credit reporting and identity theft issues. Three reports have evaluated the accuracy of credit reports:

- A PIRG report based on a Freedom of Information request to the FTC found credit reporting inaccuracies were the leading complaint to the FTC from 1991-93.

- A second key finding is that as many as one in three credit reports may contain serious errors that could cause the denial of credit, housing, insurance or even a job. This finding has been duplicated in Consumers Union studies.

Three other reports in the series have investigated the growing crime of identity theft, which affects hundreds of thousands of consumers each year. Our latest report found that victims spend two years or more removing an average of \$18,000 in fraudulent charges from their credit reports. The crime is made easier by easy access to the bits and pieces of personal information that make up a consumer's financial persona. Just last month, newspaper stories reported on how sloppy financial industry security practices enabled a high-school dropout to steal the identities of numerous celebrities:

Using computers in a local library, a Brooklyn busboy pulled off the largest identity-theft in Internet history, victimizing more than 200 of the "Richest People in America" listed in Forbes magazine, authorities say. Abraham Abdallah, 32, a pudgy, convicted swindler and high-school dropout, is suspected of stealing millions of dollars as he cunningly used the Web to invade the personal financial lives of celebrities, billionaires and corporate executives, law enforcement sources told The Post.⁵

U.S. PIRG's reports on identity theft and the hassles victims are put through by financial firms include a detailed legislative platform of reforms needed to prevent identity theft and improve the accuracy of credit reports⁶. Among the key reforms we have identified would be legislation to close the so-called credit header loophole⁷, which has been partially closed by the Gramm-Leach-Bliley financial privacy rule approved by the 7 federal financial agencies. We discuss the controversial credit header loophole below.

(2) The Need For Title V (Privacy) In Gramm-Leach-Bliley

The 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.

One of these examples involved an affiliate-sharing arrangement:

The Nationsbank/NationsSecurities case resulted in a total of \$7 million in civil penalties. Nationsbank shared detailed customer information about maturing CD holders with a securities subsidiary, which then switched the conservative investors into risky derivative funds.⁸

The second example involved a bank sharing confidential customer information with a third party telemarketer:

In June 1999 the Attorney General of Minnesota sued US Bank for sharing confidential customer “experience and transaction” information with third-party firms for telemarketing and other purposes. The telemarketer doing business with US Bank, Memberworks,⁹ had contracts with numerous other banks, as did at least one other competitor, BrandDirect,¹⁰ which has also been the subject of consumer complaints. In the U.S. Bank litigation, it was determined that not only was U.S. Bank sharing detailed customer dossiers with the telemarketer, it was also sharing account numbers. This allegedly allowed Memberworks to use deceptive telephone scripts to convince consumers to take trial offers. The consumers didn’t think they had ordered any goods, but since the bank had shared their account numbers, it turns out that they had. U.S. Bank, in 1999, signed a multi-million dollar settlement with the state of Minnesota.

In addition to providing for a nonaffiliated third-party opt-out, Gramm-Leach-Bliley included a specific provision purporting to prevent future U.S. Bank debacles. The new law prohibits sharing account numbers for marketing purposes. Unfortunately, the agencies have interpreted that law to allow sharing of “encrypted” account numbers, if there is no way for the telemarketer to “un-encrypt” the number. In our opinion, this protection is a “virtual,” or meaningless, protection, since a telemarketer could “push a button on a computer” connected to the bank and authorize the billing of a consumer who didn’t actually order anything.

In December 2000, the Minnesota Attorney General filed yet another suit, this one against Fleet Mortgage, an affiliate of FleetBoston, for substantially the same types of violations as U.S. Bank engaged in. While some consumers may presume that their credit card company, as a matter of routine, is going to attempt to pitch junky, over-priced and tawdry products such as credit life insurance, credit card protection and roadside assistance, the practice is now spreading to mortgage affiliates as well. The state’s complaint succinctly explains the problem that occurs when your trusted financial institution shares 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.¹¹

This complaint alleges that the company was providing account numbers to the telemarketer. In our view, Gramm-Leach-Bliley 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.

DO EITHER THE FCRA OR GLB MEET FAIR INFORMATION PRACTICES TESTS?

Although U.S. PIRG generally believes that consumer rights in credit reporting need to be strengthened to prevent errors and to prevent privacy invasions, the FCRA is largely based on Fair Information Practices. Companies cannot access credit reports without a permissible purpose (providing both for security and a limited form of consent), consumers have strong dispute and correction rights, and consumers have a modest private right of action. Where the FCRA largely falls short is where it interfaces with the Gramm-Leach-Bliley Act, the subject of the hearing today¹²:

1) First, the 1996 FCRA amendments exempted the sharing of “experience and transaction” information between affiliates from the definition of credit report. Under the Gramm-Leach-Bliley Act, information shared between and among affiliates (and even some third parties) for secondary purposes is not subject to either an opt-in or an opt-out. The act does provide that when financial institutions obtain so-called “other” information, that consumers must be granted a right to opt-out of sharing, even among affiliates. This right must be disclosed on GLB privacy policies.

2) Second, the 1996 amendments failed to close the so-called “credit header” loophole, established by the FTC in a 1993 consent decree with TRW (now Experian). The credit header loophole allowed credit bureaus to separate a consumer’s so-called header or identifying information – including his name, address, Social Security Number and date of birth -- from the remainder of his credit report and sell it outside of the FCRA’s consumer protections. In March 2000, the FTC held that dates of birth are used to calculate credit scores and are therefore credit-related information. It removed them from headers. The final Gramm-Leach-Bliley financial privacy rules issued later that spring by the 7 federal financial agencies defined Social Security Numbers as non-public personal information. Although the issue is currently in litigation, the agencies are, in our view, correctly interpreting the law to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out.

The Gramm-Leach-Bliley Act falls short of meeting Fair Information Practices in several areas as well.

- 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 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 GLB. 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.

THE AFFILIATE SHARING LOOPHOLE IN THE FCRA AND GLB

In 1996, when the Congress finally enacted comprehensive amendments to the FCRA, a fundamental dispute between consumer groups and the Federal Trade Commission, on one side, and the financial industry, on the other, concerned whether or not confidential consumer information shared between and among financial affiliates would be subject to the FCRA's consumer protection provisions. In 1996, the Congress chose to grant an exception to the definition of consumer report, for transaction and experience information shared between and among "companies affiliated by common control." The Congress also allowed companies to share information obtained from third parties (third parties such as the consumer herself, her credit report, and her job references) but granted the data subject a right to opt-out of the sharing of this information, even among affiliates. This right must be disclosed on GLB privacy policies.

Consumer groups contend that as financial firms get larger and contain more subsidiaries and affiliates, they may no longer need to contact credit bureaus for their own underwriting and marketing decisions. Consumers will not be able to shop around for credit (let alone for privacy policies). Gramm-Leach-Bliley can only be expected to expand the capabilities of financial services holding companies to make credit decisions without using credit bureaus. Consumers will then face credit denials, or increases in the cost of credit, without benefit of the full panoply of FCRA rights.

Basically, if affiliate A directly obtains a credit report and denies you a loan, you have full FCRA rights. If you fail to opt-out of "other" information sharing, and your credit report and application information are retained by the bank, affiliate B could make credit decisions without contacting a credit bureau. A consumer does not then have FCRA rights. If these practices grow, and if more financial institutions begin to make decisions based on their own internal profiles, or even establish internal subsidiary credit bureaus exempt from the FCRA's coverage, the effects not only on privacy, but also on competition and credit allocation, will be significant. Some consumers will not even be told they have been denied credit.

Consumer groups and other privacy proponents generally contend that information should not be shared for secondary purposes without the subject's affirmative (opt-in) consent and that this protection should apply to both affiliate and outside (third-party) transactions. During consideration of the bill that became GLB, HR 10, the full Commerce Committee, in its wisdom, chose to support by acclamation, a bi-partisan financial privacy amendment supported by privacy groups offered by Reps. Markey and Barton. The compromise amendment would have granted consumers an "opt-out" right whether confidential information was shared between affiliates or with third parties. The Markey-Barton amendment would have given consumers the right to an opt-out that would have protected all their financial information from being used for secondary purposes by either an affiliate or any third party. As Representative Barton stated on the floor during consideration of HR 10:

The question I ask this body and this country is: If we are concerned about the selling and sharing of information to third parties, should we not be just as concerned about the selling, sharing, transmitting, or accessing that information inside of these affiliates if there are going to be dozens or hundreds of these affiliates? ... Until we solve the riddle

of handling information within the affiliate structure, we do not have privacy. We do not have privacy.¹³

Unfortunately, neither the Banking Committee, nor the House leadership, nor the Senate, agreed. The Commerce Committee privacy amendment was not passed in the Banking Committee and was not even considered on the floor of either House, even though it passed the full Commerce Committee.

The final version of Gramm-Leach-Bliley defines non-public personal information that is to be protected under the act. It then bifurcates third party companies into two groups. The first, affiliated third parties, are treated as affiliates for information-sharing purposes. Companies can share experience and transaction information (including non-public personal information) between and among both affiliates and affiliated third parties, which may be providing services on behalf of the bank, regardless of a consumer's opt-out preference. However, after the effective date (1 July 2001) of GLB, such information can only be shared with nonaffiliated third parties if the consumer has been granted notice and been given an opportunity to opt-out. There are two primary implications of this limited protection. First, consumers will have the ability to limit access by third party telemarketers to their confidential financial information. Second, they may be able to protect their Social Security Numbers from secondary use by information brokers.

THE LAWSUITS OVER THE NARROWING OF THE CREDIT HEADER LOOPHOLE

Consumer and privacy groups strongly contend that easy access to consumer identifying information leads to stalking and identity theft. Even if it did not, groups strongly support restrictions on the secondary use of Social Security Numbers, which were never intended as a national identifying number yet form the key for establishing someone's location or identity. In other areas, such as Drivers' License privacy, the Congress has sought to narrow the availability of Social Security Numbers.¹⁴ In the 106th Congress, Social Security Number protection legislation named for Amy Boyer, 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, primarily to customers of the Individual References Services Group. IRSG member companies include credit bureaus and other information firms engaged in the sale of non-public personal information to locator services, debt collectors, information brokers, private detectives and others.¹⁵

In 1993, the Federal Trade Commission 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. 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.¹⁶ The FTC's theory was that credit headers included information that ostensibly did not bear on creditworthiness and therefore was 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 from the remainder of his credit report and selling it outside of the FCRA's consumer protections. Although the information, marketing and locator industries contend that header information is derived from

numerous other sources, in reality, the primary source of the most accurate and best credit header data is likely information provided by financial institutions with monthly credit updates.

In March 2000, the FTC held that dates of birth are credit-related information and removed them from headers.¹⁷ The final Gramm-Leach-Bliley financial privacy rules issued later that spring by the 7 federal financial agencies defined Social Security Numbers as non-public personal information. Although the issue is currently in litigation, the agencies are, in our view, correctly interpreting the law. Since Social Security Numbers are held to be non-public personal information, the rule acts to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out. 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 redisclosure 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]¹⁸

In their lawsuits filed to block the inclusion of Social Security Numbers in the Gramm-Leach-Bliley definition of non-public personal information, the credit bureaus and other IRSG members the firms make any number of kitchen-sink arguments against the rule.¹⁹ Among the most important are their claims that the Gramm-Leach-Bliley Act does not affect the FCRA, that the breadth of the agencies’ rules goes beyond statutory intent, and that the agencies should not be granted any deference under the Supreme Court’s Chevron²⁰ test.

First, the firms argue that Gramm-Leach-Bliley includes a savings clause (Section 6806) that the law does not “modify, limit, or supersede the operation of the Fair Credit Reporting Act.” This view is without merit, since no part of the Fair Credit Reporting Act allows the sale of credit headers. As the FTC points out in its preamble to the rule, “To the extent credit header information is not a consumer report, it is not regulated by the FCRA and a prohibition on its

disclosure by a consumer reporting agency consistent with the statutory scheme of the G-L-B Act in no way modifies, limits or supercedes the operation of the FCRA.²¹”

Second, the firms argue that the agencies went too far in defining non-public personal information and that the rule should be rejected on these grounds. They further argue that the agencies are not entitled to deference in their statutory interpretations under the Chevron test²². The consumer groups strongly disagree with the firms on these counts. First, it was very clear from the legislative history of GLB that the Congress intended confidential information provided to financial institutions as a condition of obtaining an account should be construed as non-public personal information. Second, seven separate federal financial agencies, all with expertise in financial industry matters, concurred on identical regulations.

Based on the record, then, if anything, the seven agencies that issued an identical joint rule agencies should be granted sweeping Chevron deference “ultra.” The seven agencies have done an admirable job of determining that GLB requires the deletion of Social Security Numbers from credit headers, unless consumers are given notice and an opportunity to opt-out. When credit bureaus sell credit reports, they are entitled to the FCRA savings clause of GLB. When credit bureaus sell credit headers, they are clearly nonaffiliated third parties selling non-public personal information. Disappointingly, rather than comply with Congressional intent, the firms have chosen to roll the dice in the courts.

ASSAULT ON STATE LAWS AND THE SO-CALLED “COSTS” OF PRIVACY

The 1996 amendments to the Fair Credit Reporting Act partially preempt the right of the states to enact stronger laws, especially in the area of prohibiting affiliate sharing, until 2004. Although Gramm-Leach-Bliley, overall, is sweepingly preemptive, Title V includes a state law savings clause, the so-called Sarbanes amendment that allows states to enact stronger privacy laws (Section 6807). We disagree with industry groups that this provision’s applicability to affiliate sharing is trumped by Title V’s FCRA savings clause. Unfortunately, the financial industry has not only sent lobbyists out en masse to oppose enactment of stronger state financial privacy laws under consideration in numerous states, it has also sent them out to attack existing laws. This week, North Dakota apparently was convinced to gut an existing financial privacy law and Vermont is under extreme pressure to do so as well. We urge the states to reject the financial industry’s unfounded and blackmail-like claims that they stop selling products in your state unless you accede to their wishes and eviscerate your consumer laws.

The financial services and other information industries have also unleashed a massive public relations assault purporting that privacy costs too much money and, incredibly, according to some news stories, may bring down the economy. U.S. PIRG intends to review the industry-funded studies that form the alleged basis for these claims in greater detail. We urge the committee to evaluate the claims made in these industry-funded studies in great detail before acting on them, if at all. The American people have demonstrated strong support for strong privacy protections. In our view, the costs of not protecting privacy – increased identity theft and stalking, sale of unsatisfactory telemarketed products, loss of the right to be left alone – easily outweigh these purported costs to industry. We will provide the committee with more analysis as it becomes available.

CONCLUSION

We appreciate the opportunity to testify before you on the important matter of financial privacy. Although neither the Fair Credit Reporting Act nor the Gramm-Leach-Bliley Act go as far necessary to protect consumer privacy, the laws together play an important role in establishing a minimal framework of financial privacy protection. We look forward to working with the committee to strengthen the laws.

¹ See the "Privacy Law Sourcebook, 2000: United States Law, International Law and Recent Developments," by Marc Rotenberg, Electronic Privacy Information Center, for a comparison of all important privacy laws.

² Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998 <<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>>

³ 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: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 50-51.]

1. Collection limitation. There must be no personal data record keeping systems whose very existence is secret.

2. Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

⁴ Consumer groups oppose legislation, HR 3408, introduced in the 106th Congress (and expected to be re-introduced) by Rep. Pete Sessions to exempt workplace misconduct reports from the FCRA. We recognize that an unintended consequence of the 1996 amendments to the FCRA unwisely gives investigatory subjects a warning that they are under investigation. The solution is not to exempt workplace investigations, a major area of abuse of workers, from the FCRA. See 4 May 00 testimony of the National Consumer Law Center and U.S. PIRG, with an appendix provided by the AFL-CIO, that details the problem: <<http://www.house.gov/financialservices/5400sau.htm>>

⁵ See New York Post, 20 March 2001, "HOW NYPD CRACKED THE ULTIMATE CYBERFRAUD" <http://dailynews.yahoo.com/hix/nypost/20010319/lo/how_nypd_cracked_the_ultimate_cyberfraud_1.html>

⁶ See "Nowhere To Turn: A Survey Of Identity Theft Victims," May 2000, CALPIRG, U.S. PIRG and the Privacy Rights Clearinghouse, for the latest version of the platform: <<http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>>

⁷ In the 106th Congress, bi-partisan legislation approved by the Ways and Means Committee (HR 4857, Shaw-Matsui-Kleckza) would have eliminated Social Security Numbers from credit headers. Several other bills would close the credit header loophole.

⁸ See SEC Release No. 7532 And Release No. 39947, May 4, 1998, Administrative Proceeding Against NationsBank, NA And NationsSecurities, File No. 3- 9596, In The Matter Of : Order Instituting Cease-And- Desist Proceedings Pursuant To Section 8a Of The Securities Act Of 1933 And Sections:15(B)(4)

And 21c Of The Securities Exchange Act Of 1934 And Findings And Order Of The Commission. See <<http://www.sec.gov/enforce/adminact/337532.txt>> (Note, total civil penalties of nearly \$7 million includes fines paid to other state and federal agencies, as well as to the SEC.) From the order:

“NationsBank assisted registered representatives in the sale of the Term Trusts by giving the representatives maturing CD lists. This provided the registered representatives with lists of likely prospective clients. Registered representatives also received other NationsBank customer information, such as financial statements and account balances. These NationsBank customers, many of whom had never invested in anything other than CDs, were often not informed by their NationsSecurities registered representatives of the risks of the Term Trusts that were being recommended to them. Some of the investors were told that the Term Trusts were as safe as CDs but better because they paid more. Registered representatives also received incentives for their sale of the Term Trusts.”

⁹ On Friday, 16 July 1999, the Minnesota Attorney General filed suit against Memberworks. At least four other states (Florida, California, Washington and Illinois) are investigating the firm. See The Washington Post, “Telemarketer Deals Challenged in Suit, Sale of Consumer Financial Data Assailed,” by Robert O’Harrow Jr, Saturday, July 17, 1999; Page E01.

¹⁰ For articles on BrandDirect and Chase Manhattan, see for example, The Seattle Post-Intelligencer, “You may be a loser -- buying something you didn’t want”, by Jane Hadley, Thursday, April 8, 1999 or Newsday, “ Company Had Her Number / Woman discovers to her surprise card issuer gave out account data” by Henry Gilgoff, 9 May 1999.

¹¹ 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>

¹² FCRA also preempts state laws in most respects, until 2004, and fails to provide free access to credit reports except in limited circumstances. We oppose these two provisions.

¹³ Floor debate on HR 10, Congressional Record, Page H5513, 1 July 1999.

¹⁴ See enacted 2000 amendments to the Drivers Privacy Protection Act by Senator Shelby. For more information about privacy invasions caused by access to Social Security Numbers, see the new book, “War Stories III,” by Robert Ellis Smith, Publisher, Privacy Journal, <<http://www.privacyjournal.net>>

¹⁵ See the U.S. PIRG Fact Sheet, “Why The Amy Boyer Law Is A Trojan Horse” at <<http://www.pirg.org/consumer/trojanhorseboyer.pdf>>

¹⁶ The industry has since established an association, the Individual References Services Group, which purports to manage a voluntary self-regulation that regulates sale of non-public personal information included in credit headers to what it terms “authorized commercial and professional users.” In our view, information brokers can easily slip through IRSG’s net.

¹⁷ See Trans Union Order, March 2000.

¹⁸ 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>>

¹⁹ Several lawsuits have been filed, including by Trans Union, Individual References Services Group, and other credit bureaus. Although cross-motions for summary judgments have been filed by both sides in the U.S. District Court for the District of Columbia, no oral argument has been scheduled.

²⁰ Chevron USA vs. Natural Resources Defense Council, 467 US 837 (1984).

²¹ Pages 81, Federal Trade Commission, 16 CFR Part 313, Privacy Of Consumer Financial Information, Final Rule <<http://www.ftc.gov/os/2000/05/glb000512.pdf>>

²² See Pages 14-18, Memorandum in Support of Trans Union LLC’s Motion For Summary Judgment, Trans Union vs. Federal Trade Commission, Civil Action No 1:00 CV 02087 (ESH), 1 Nov 00.