

FINANCIAL PRIVACY AND CONSUMER PROTECTION

HEARING
BEFORE THE
COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE
ONE HUNDRED SEVENTH CONGRESS
SECOND SESSION
ON
THE GROWING CONCERNS OVER THE WAY CONSUMERS' PERSONAL
AND FINANCIAL INFORMATION IS BEING SHARED OR SOLD BY THEIR
FINANCIAL INSTITUTIONS

SEPTEMBER 19, 2002

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



U.S. GOVERNMENT PRINTING OFFICE

90-080 PDF

WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

PAUL S. SARBANES, Maryland, *Chairman*

CHRISTOPHER J. DODD, Connecticut	PHIL GRAMM, Texas
TIM JOHNSON, South Dakota	RICHARD C. SHELBY, Alabama
JACK REED, Rhode Island	ROBERT F. BENNETT, Utah
CHARLES E. SCHUMER, New York	WAYNE ALLARD, Colorado
EVAN BAYH, Indiana	MICHAEL B. ENZI, Wyoming
ZELL MILLER, Georgia	CHUCK HAGEL, Nebraska
THOMAS R. CARPER, Delaware	RICK SANTORUM, Pennsylvania
DEBBIE STABENOW, Michigan	JIM BUNNING, Kentucky
JON S. CORZINE, New Jersey	MIKE CRAPO, Idaho
DANIEL K. AKAKA, Hawaii	JOHN ENSIGN, Nevada

STEVEN B. HARRIS, *Staff Director and Chief Counsel*

LINDA L. LORD, *Republican Staff Director*

DEAN SHAHINIAN, *Counsel*

DARIS D. MEEKS, *Republican Counsel*

MARK F. OESTERLE, *Republican Counsel*

SARAH E. DUMONT, *Republican Professional Staff*

JOSEPH R. KOLINSKI, *Chief Clerk and Computer Systems Administrator*

GEORGE E. WHITTLE, *Editor*

C O N T E N T S

THURSDAY, SEPTEMBER 19, 2002

	Page
Opening statement of Chairman Sarbanes	1
Opening statements, comments, or prepared statements of:	
Senator Shelby	2
Senator Stabenow	3
Senator Akaka	26
Senator Corzine	27
Senator Carper	41
WITNESSES	
William H. Sorrell, Attorney General, The State of Vermont	4
Prepared statement	46
Fred H. Cate, Professor of Law, Indiana University School of Law	8
Prepared statement	53
John C. Dugan, Partner, Covington & Burling; on behalf of the Financial Services Coordinating Council	11
Prepared statement	57
Mike Hatch, Attorney General, The State of Minnesota	14
Prepared statement	62
James M. Kasper, Member, House of Representatives, The State of North Dakota	17
Prepared statement	65
Phyllis Schlafly, President, Eagle Forum	21
Prepared statement	69
Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Re- search Group; on behalf of: Consumer Action, Consumer Federation of America, Consumer Task Force on Automotive Issues, Consumers Union, Electronic Privacy Information Center, Identity Theft Resource Center, Junkbusters, Inc., Privacy Rights Clearinghouse, Private Citizen, Inc., and U.S. Public Interest Research Group	23
Prepared statement	72

FINANCIAL PRIVACY AND CONSUMER PROTECTION

THURSDAY, SEPTEMBER 19, 2002

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:07 a.m. in room SD-538 of the Dirksen Senate Office Building, Senator Paul S. Sarbanes (Chairman of the Committee) presiding.

OPENING STATEMENT OF CHAIRMAN PAUL S. SARBANES

Chairman SARBANES. The hearing will come to order.

This morning, the Committee meets to hear testimony on the issue of financial privacy and consumer protection. At the very outset, I want to acknowledge the interest and the contribution which Senator Shelby has made regarding this issue and I am pleased to be working with him on it.

Senator SHELBY. Thank you, Mr. Chairman.

Chairman SARBANES. During the past few years—even longer, actually—there have been growing concerns over the way consumers' personal and financial information is shared or sold by their financial institutions. In 1999, when we did the major revision of the structure of the financial industry, after considerable debate, we enacted certain Federal privacy protections, although many perceived them as not to be fully adequate to the challenge, and therefore, financial privacy remains a critical issues.

The amount of sensitive personally identifiable financial information that, under current Federal law, can be circulated is vast. It includes savings and checking account balances, certificates of deposit maturity dates and balances, any check which an individual writes, any check that is deposited into a customer's account, stock and mutual fund purchases and sales, life insurance payouts, and other data. The universe of consumer data that the financial institutions can collect, warehouse, and then either share or sell is increasingly growing, some think at a very rapid pace. Modern technology makes this sharing cheaper, quicker, and easier than ever before. I think the real issue is that much of this is done without the knowledge or the approval of the customer regarding the specific information being transferred or the specific affiliated or nonaffiliated company to whom it is either being sold or shared.

Financial privacy is in many respects a fundamental right that all consumers should enjoy. And obviously, if that is the case, if it is not adequately protected, we can have abuses.

Recent reports and surveys indicate the public's ongoing concerns. Dr. Alan Westin of Columbia University, who heads Privacy and American Business, wrote this year: "Both on and off the Internet, consumers are more concerned about privacy today than they have been at any point over the past 2 years." A survey published this year by that group and sponsored by the AICPA and Ernst & Young found that 79 percent of respondents agreed with the statement: "Consumers have lost all control over how personal information is collected and used by companies." The same survey found that the number of respondents who disagreed with the statement: "Existing laws and organizational practices provide a reasonable level of protection for consumers today." That was the statement, that existing laws and practices provided a reasonable level of protection. The number disagreeing with that statement has gone from 38 percent in 1999 to 62 percent in 2001.

We obviously need to address the issue of whether consumers should have the right to choose whether his or her bank or other financial institution may circulate private financial information to others for purposes that the consumer may never have originally intended.

At today's hearing, we will hear testimony with respect to a number of questions: Do consumers continue to be concerned about their financial privacy, the privacy of nonpublic personally identifiable data held by financial institutions? What types of concerns do consumers have about the possible uses of their financial information? Are the minimum financial privacy protections in Federal law adequate to meet the consumer's concerns? What recommendations would panelists make to the Committee regarding financial privacy protection?

We have a number of very able witnesses with us this morning. In a sense, I apologize for the breadth of the panel, but we had many people that we wanted to hear from. I think what I will do, in view of that, is I will introduce each witness as we come to them, rather than introducing them all here at the outset because, by the time we get to the last witness, they may have forgotten what was said about them.

[Laughter.]

So before I begin the process of going to the witnesses, we thank all of you for coming today, we very much appreciate your participation, I yield to my colleagues for any opening remarks.

First, I turn to Senator Shelby.

STATEMENT OF SENATOR RICHARD C. SHELBY

Senator SHELBY. Thank you, Mr. Chairman. Thank you for calling this hearing. And I also want to thank you for your long-time interest and work in this area. We worked together on a number of initiatives dealing with financial privacy and I believe we will continue to work those issues because the more I see and talk to the American people, most of them do not realize what is going on yet. But they are learning. And hearings like this certainly help.

Mr. Chairman, the subject of financial privacy is one that is very important to all of us and requires the Committee's thorough consideration, as you realize.

I want to thank the witnesses for taking the time to come here to share their views and experiences with us. And I look forward to hearing from all of you.

This issue of privacy is not a new one. In one way or another there has been an ongoing debate about privacy since the founding of this country. However, the issue has clearly evolved over time as a range of specific incidents and general trends have raised public concerns about new or different threats to our privacy. Where once only the Government possessed the ability to obtain and the means to exploit vast amounts of personal data, technology now makes it possible for just about anyone to collect, to store, to sell, or to do just about anything that they want to with a lot of our private items.

I believe that the existence of such capabilities requires that we carefully, here in the Congress, examine the pros and cons of its use relative to the disclosure of personal information. Furthermore, as we move forward, I think it is extremely important that we continue to pay close attention to the significant role that technological capability is going to play in this debate. Consumer and industry demand for faster and more reliable information exchange is only going to increase. As technological capabilities are expanded to keep up, new and unforeseen issues concerning the use of sensitive personal financial information I believe will continuously arise.

While it may not be possible to develop rules that deal with every possible scenario involving the use of confidential financial information, I believe the American people will demand that we establish some basic principles that will guide our future efforts.

In order to do this I believe that it is important for this Committee, the Banking Committee, to draw from a broad range of perspectives in considering the basic questions regarding the various Federal laws touching on financial privacy. For instance: Are such laws effective? Are they targeted to consumer concerns? Do consumers even understand them? I am going to ask that again: Do consumers even understand them? Are they in sync with today's marketplace? What restrictions do they place on business activity?

Additionally, in light of the fact that the States play an important role in this area, I think it is also essential for us to gain a better understanding of their efforts and to consider some basic questions about their activities. For instance: Do State officials have a greater perspective or awareness regarding the trends or concerns about financial privacy? What value is provided by preserving a State legislative role, thanks to Senator Sarbanes? What value is provided by preserving strictly a State enforcement role? How does State activity impact the financial services industry?

It is my hope that this is just the first, Mr. Chairman, of what I hope are a whole series of opportunities to consider this issue. I look forward to a productive and informative dialogue here and I thank you for this hearing.

Chairman SARBANES. Thank you very much, Senator Shelby.
Senator Stabenow.

STATEMENT OF SENATOR DEBBIE STABENOW

Senator STABENOW. Thank you, Mr. Chairman. And to you and to Senator Shelby, thank you for your leadership.

I think this is one of the most important issues that we face as we move forward at this time, and I appreciate the fact that we have so many people willing to share their expertise with us today.

This is a topic that, in our increasingly sophisticated world, is one that consumers are extremely concerned about, as has been indicated. We know that our financial decisions can be recorded, analyzed, shared, and sold, and consumers want to know that they have a basic level of privacy. We all want to know that we have that basic level of privacy.

When we passed the privacy provisions of Gramm-Leach-Bliley, we were breaking new ground. We gave the public a certain degree of control, but not as much as many would have liked. And since the Act was passed in 1999, the regulators have had the opportunity to set standards, as we know, and financial institutions have been complying with the law.

Now it is appropriate to reflect on that legislation and how it is being implemented and where we should go from here. Is it sufficient? Is it being implemented effectively? As Senator Shelby said, do consumers really understand their privacy rights? Are the annual financial privacy disclosures effective or simply thrown away with all of the other things that come in the mail? What are regulators doing to make sure that these disclosures meet the spirit of the law?

I also believe it is important to look at States, as Senator Shelby was mentioning. I know there have been a number of serious debates going on in States. In particular, there has been a lot of focus on North Dakota and California. I suspect the discussions will continue, from Sacramento to my hometown of Lansing, Michigan, to Annapolis, all across the country, this will become more and more of a debate and discussion, as it should.

So, Mr. Chairman, thank you again for what I think is a very important hearing. I hope this helps us lay a foundation as we move into the next Congress to focus on this issue, which I know is of deep, deep concern to the American public.

Chairman SARBANES. Thank you very much, Senator Stabenow.

We will now turn to our panel. We will first hear from Attorney General William Sorrell, who has been the Attorney General of the State of Vermont since 1997. Attorney General Sorrell is the Vice President of the National Association of Attorneys General and Co-Chair of its Consumer Protection Committee. Earlier, he served as Vermont's Secretary of Administration.

Mr. Attorney General, we are very pleased to have you here.

**STATEMENT OF WILLIAM H. SORRELL
ATTORNEY GENERAL, THE STATE OF VERMONT**

Mr. SORRELL. Thank you very much.

Chairman SARBANES. I think if you pull that microphone close to you, it will be helpful to all of us.

Mr. SORRELL. Good morning.

Chairman SARBANES. That is better, yes.

Mr. SORRELL. Thank you for inviting me to speak with you today on the important issue of financial privacy.

The State Attorneys General are grateful for the work of this Committee on this important consumer issue and we especially

want to commend Chairman Sarbanes and Senator Shelby for working so hard to address these issues in a bipartisan fashion.

As this panel of witnesses demonstrates, concerns about the privacy of consumers' financial information is neither a Democratic issue, nor a Republican issue. It is not a liberal issue, nor a conservative issue. Rather, it cuts across traditional party and philosophical lines to touch all of us who are concerned about protecting our citizens.

The Chairman did indicate that I am the Vice President of the National Association of Attorneys General. But I want to make clear for the record that I am here for myself and representing my Office of Attorney General for the State of Vermont.

I am not here purporting to speak for the entire National Association of Attorneys General.

Chairman SARBANES. As they say on those ads that they put in the paper when they get all those academics to sign and give their institutions, just for the purpose of identification.

[Laughter.]

Mr. SORRELL. Thank you very much, Mr. Chairman.

[Laughter.]

Along with my esteemed colleagues on this panel, I am here today to tell you that the privacy provisions of Gramm-Leach-Bliley are not working. Although this Committee worked hard to enact provisions to eliminate the abusive practices that were uncovered by the State Attorneys General in 1999, in fact, these practices are continuing largely unabated.

I strongly recommend that this Committee undertake a thorough examination of the effects of Gramm-Leach-Bliley and the related regulations implemented by the Federal regulators in order to determine whether the law, as interpreted by the Federal agencies, carries out your intent. I believe you will find that it does not do so. I also believe you will want to enact strong provisions to correct problems that have arisen under Gramm-Leach-Bliley.

What are some of these problems that consumers are facing?

First and foremost, the unfortunate telemarketing practices that were uncovered in 1999, by Minnesota Attorney General Hatch are continuing. The U.S. Bancorp case demonstrated that major financial institutions were facilitating abusive telemarketing by selling their customers' account numbers and other nonpublic personal financial information to vendors, who then turned around and sold consumers memberships in travel clubs, gardening clubs, esoteric insurance products, often through improper use of information provided by the financial institution.

This Committee wanted to put a stop to such practices, and so prohibited financial institutions from sharing account numbers. But the Federal agencies responsible for interpreting the law allow financial institutions to share or sell encrypted account numbers or other unique identifiers, thereby giving the telemarketers essentially the same access to consumers' accounts as before.

So just as was the case prior to Gramm-Leach-Bliley, an eager telemarketer, paid on commission, is able to convert a consumer's ambiguous statement of interest into a purchase. The telemarketer simply informs the financial institution that a charge should be processed on that consumer's account. The telemarketer doesn't

need the actual account number because the bank will convert the encrypted number or unique identifier into the account number for processing the charge. The consumer doesn't know how the charge appeared on her account since she never gave out her account number. In many instances, she doesn't even know she made a purchase.

This Committee should undertake a thorough investigation of these continuing abusive telemarketing practices and afford greater protection to consumers in this regard.

Gramm-Leach-Bliley is also not working because the notices required under the law are fundamentally incomprehensible to too many consumers. My written testimony fully covers the surveys and studies that demonstrate the dense writing of these notices, as well as the correspondingly high reading levels required to understand them.

I thought, and with the Committee's indulgence, that I might just take a moment to read just one paragraph from one of these notices. This should serve to give the Committee a flavor of what consumers face in trying to decipher these notices and the excerpt I will read is from the American Bankers Association model, Gramm-Leach-Bliley privacy policy notice, that it sent out to its members for use in their notices.

And in that notice, and I believe the average American household received roughly eight or more of these notices, under the heading, What Information We Disclose, if you get down in the body of the notice, here is what you find:

We may disclose nonpublic personal information about you to the following types of "affiliates" (i.e., companies related to us by common control or ownership) and "nonaffiliated third parties" (i.e., third parties that are not members of our corporate family). Financial service providers, such as mortgage bankers, security brokers-dealers, and insurance agents. Nonfinancial companies, such as retailers, direct marketers, airlines and publishers. And others, such as nonprofit organizations.

If you prefer that we not disclose nonpublic personal information about you to such nonaffiliated third parties [with respect to this loan or account], you may opt-out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt-out of disclosures to nonaffiliated third parties, you may call the following toll-free number.

I hope I have made my point.

It stretches credulity to think that average consumers can readily work their way through these obtuse notices and reach a basic understanding of their rights to control the sharing of financial information. And then to make informed choices in this regard.

This is exactly why the Attorneys General of 44 of the States and territories recently called on the Federal regulatory agencies to create standard notices to require much simpler language so that consumers can more readily understand the notices.

This Committee should give serious consideration to requiring standard privacy notices similar to the nutritional notices that are required in the Federal Nutritional Labeling and Education Act.

This Committee had the wisdom to ensure that States would have the authority to go further than Gramm-Leach-Bliley to enact more protective laws governing financial privacy.

We hope the Committee will continue to allow States to protect their citizens as they see the need to do so. Indeed, several States had enacted more protective laws governing financial privacy prior to the adoption of Gramm-Leach-Bliley. Because consumers contin-

ued to be very concerned about the protection of their personal financial information, States have continued to adopt laws that are more protective than Federal law.

Currently, there are six States that have enacted laws that require some form of opt-in before financial information can be shared by banks, and 14 States have enacted laws that require some form of consumer consent before financial information can be shared by insurance companies.

As my co-panelist, Representative Kasper, will describe, North Dakota voters recently adopted a referendum reversing the State legislature's repeal of that State's opt-in law, thereby putting that State's banking opt-in law back on the books. In addition, two California localities, San Mateo County and Daley City, have recently adopted ordinances requiring affirmative consumer consent before financial information may be shared.

These State and local laws are a reaction to the problems associated with Gramm-Leach-Bliley and an effort by these governments to exercise the power given them by this Committee under Section 507, to provide consumers with protections greater than those afforded under Federal law.

The sharing of financial information among corporate affiliates remains another real concern. Should a consumer who opens an account with Citibank, for example, expect that, for purposes of "preacquired account marketing," her account number will be shared with Travelers Insurance or any of the other 2,761 affiliates within Citigroup? The number and the breadth of affiliates currently associated with some of the country's major financial institutions is truly astounding.

In addition to the Citigroup's 2,761 affiliates, the web site of the Federal Reserve lists 1,476 corporate affiliates for Bank of America, and 871 affiliates for KeyCorp, which is considered to be a mid-size bank.

A perusal of these corporate affiliate lists demonstrates that these holding companies appear to be involved in widely disparate activities, including insurance, securities, international banking, real estate holdings and development, and equipment leasing.

So a consumer holding a credit card with the lead bank or an insurance policy with a major insurer in any of these affiliate groups would not expect that his or her account number would be spread throughout the corporate affiliate structure for the purpose, not of servicing the consumer better, but of marketing products to the consumer.

This Committee should require that financial institutions give consumers an effective choice before nonpublic personal financial information can be shared among affiliates.

Moreover, the Congress should direct that the standard financial privacy notices to be created by the Federal regulatory agencies contain a standard format for information about affiliate-sharing practices and consumers' choices to prevent such sharing.

Mr. Chairman, I referred to the following documents* in my written and oral testimony. I would like to have them submitted into the record: Affiliate lists for Bank of America, Citigroup, and

*Held in Committee files.

KeyCorp; a report from my office and our Department of Banking and Insurance; an interim report to the Vermont legislature on financial privacy; the final of such report; and the American Bankers Association sample privacy notice. I hope those and my written testimony will be accepted into the record.

Chairman SARBANES. They will be held in Committee files.

Mr. SORRELL. Thank you very much for this opportunity.

Chairman SARBANES. Thank you very much. We very much appreciate hearing from you.

We will now turn to Fred Cate, Professor of Law at the Indiana University School of Law in Bloomington, Indiana, and a Senior Policy Advisor at the Hunton & Williams Center for Information Policy Leadership.

Professor Cate.

**STATEMENT OF FRED H. CATE
PROFESSOR OF LAW
INDIANA UNIVERSITY SCHOOL OF LAW**

Dr. CATE. Thank you very much, Mr. Chairman, distinguished Members of the Committee. I appreciate the opportunity to be here.

I should offer the same qualification as my distinguished colleague, which is, of course, that my comments do not reflect the views of Indiana University.

One would like to think that the University would have the good sense that they would.

[Laughter.]

But in any event, the University would want me to clarify that they do not necessarily.

There is much to say, but I will do my best to limit myself to four points and try to make those as briefly as possible.

First, there is no doubt but what consumers are concerned about financial privacy. It seems like there is no room to even debate that question. I think the issue is what do we make of that concern and what would this Committee and the Congress do in response to that concern?

I, for one, do not find that concern tremendously surprising. Consumers should be concerned about financial privacy. They should be concerned about privacy in many areas because, frankly, many of the most effective and, in some cases, the only effective, steps to protect an individual's privacy are individual actions. They are not protections afforded by law. They are not protections afforded by policies or technologies, but, rather, the things that an individual himself or herself will do.

So given that we have just had a deluge, twice now, of more than two billion privacy notices, given the attention given this issue in the press, it would, I think, be surprising if there weren't consumer concern about this issue, and I think that concern is largely healthy.

Clearly, it is not healthy to the extent that it represents lack of knowledge about either banking practices or the law, and I will return to this in my conclusion.

Second, in addition, however, to looking at the presence of consumer concern, we also have to look at consumer action. And what we know is that in response to tens of thousands of financial insti-

tutions, mailing billions of privacy notices, the opt-out rates seem to be consistently less than 5 percent. Many institutions report opt-out rates of 1 percent or less.

This is true, by the way, not only in financial privacy. This is true with the FCRA opt-out provisions. This is true for the DMA's opt-out provisions. This is true for many companies that report what their specific industry opt-out rates are. A low response rate is very consistent.

So before encouraging the Congress to adopt new laws or more restrictive privacy laws, it seems important to first understand why consumers aren't taking advantage of the rights that they currently have under existing law. Before giving new rights, why are the current rights not being used?

Third, another reason for concern about going forward with more restrictive privacy laws on either the State or Federal level is, of course, that information serves many valuable, irreplaceable functions in this economy and in the society.

This point seems so obvious that I do not want to belabor it here. It has been much written about. And probably the most articulate spokesperson coming from the Federal Reserve Board. Let me just offer one quote from Governor Gramlich: "Information about individual's needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, "the more accurately and efficiently will the economy meet those needs and preferences."

This seems particularly true in the case of affiliate-sharing. The number of affiliates which have been referred to certainly could give one pause. But I think it is worth noting that research shows that companies do not create affiliates just for the opportunity to create affiliates, that affiliate relationships are often driven by tax or liability issues, by regulatory requirements, by any number of State licensing issues.

The question then of whether affiliate-sharing of information should be permitted or restricted would necessarily, if made a legal issue, require that companies describe in detail their affiliate relationships to their customers.

It is difficult to imagine how even the best-intentioned privacy notice, if required to describe those relationships in detail, could ever be comprehensible to anybody, to anybody here or to anyone likely to receive those notices.

Interfering with those benefits of information flows, of course, impose costs on consumers. There are also additional costs, however, imposed by privacy laws, and I think this Committee is well aware of and I think that this is very relevant to the question of whether more restrictive privacy laws seem appropriate.

We know that the cost of complying with Gramm-Leach-Bliley has been measured in the range of \$2 to \$5 billion a year for financial institutions, cost that are, of course, passed on, either to the customers directly or to shareholders, and indirectly to customers.

These costs, however, are much greater. Experience and research in this area are consistent and, without exception, show that costs are much greater when a privacy law imposes a greater restriction on information-sharing, for example, opt-in. In fact, most of the available research on opt-in statutes in practice show that if they

require contacting a consumer after the consumer has engaged in the transaction, after the consumer has opened the account, after the consumer has sought service, an opt-in statute effectively works as a ban on information flows that, in practice, the result is no consent and no opportunity to share information.

I want to be clear, however.

I think that those costs should be measured not only in dollars, but also would encourage the Committee and would direct the Committee's attention to the other types of costs that that can impose. And here research is particularly informative.

Even a subject like informing consumers about opportunities, marketing, which seems to meet with very little support in any public forum today, nevertheless, is of obvious importance to many consumers and especially those less likely to have, for example, financial advisors, less likely to be well-endowed financially.

We know, for example, that greater information restrictions disproportionately affect poor and also people located away from urban centers. This, of course, is also especially true with opt-in.

I have mentioned in my written testimony and I will not belabor now a case study that economist Michael Staten and I did of just one financial institution, MBNA Corporation, and what the cost of opt-in would be on MBNA's customers. Those costs are significant and I would encourage the Committee to pay close attention to the consistent evidence of how great those costs can be, especially since, to use MBNA's numbers for the period of the case study, 2000 to 2001, fewer than one quarter of 1 percent of MBNA customers had opted out. So imposing any additional costs, given that fewer than one quarter of 1 percent had found the protection necessary, would seem dubious, at best.

Remember, and I will quote here Alabama Attorney General Bill Pryor, it is customers and individuals who ultimately "pay the price of either higher prices for what they buy or in terms of a restricted set of choices offered them in the marketplace, for restrictive privacy laws."

Finally, I think it is important to keep in mind the larger context in which this debate is taking place.

Gramm-Leach-Bliley passed in 1999 and notices were required to be mailed, the first set, by July 1, 2001. Only 14 months has passed during that time and we have seen significant changes and developments that would strike me as very positive in that time.

While the issue of consumer confusion has already been noted, I think it is important here to return to the question of why notice is needed to be improved, why the developments of the past 14 months, in fact, warrant approval rather than disapproval from this Committee.

Remember the law itself is very complex. If you have ever tried to explain it to anyone, you appreciate how complex the law is. The terms used, for example, in the ABA model notice that was previously read, largely came from the law and from the implementing regulations.

If you want simple requirements to be explained to consumers, you will have to enact simple requirements. And in this area, that is very, very difficult. So, for example, distinctions between consumers and customers, which are so important to the law, do not

make much sense to ordinary people. It is difficult to understand these.

It should also be noted that clarity seems to be very much in the eye of the beholder.

I had the experience on June 18, 2001, of appearing before the California General Assembly Committee on Banking and Finance, where the Committee Chairman lauded American Express for the clarity of its notice. In fact, he passed out copies to everyone in the audience, so, as he said, industry representatives could live up to the model set by American Express.

Three weeks later, on July 9, 2001, *USA Today* cited American Express' notice as one of the least comprehensible it had read.

There is much going on. There are market responses. We are seeing banks and other financial institutions offering privacy-related cards and other privacy-related services. We are seeing the quality of notices being improved, the Federal Trade Commission working to improve that quality. We are seeing new types of privacy protections, many from the States, such as do-not-call lists.

In the absence of evidence of harms not being addressed by the current law, not just Gramm-Leach-Bliley, but the full range of Federal and State financial privacy laws, it seems inappropriate, or at least premature, to move forward with more restrictive privacy requirements.

Thank you.

Chairman SARBANES. Thank you very much, sir.

Now, we will hear from John Dugan, appearing today, I think it is fair to say, actually, representing the Financial Services Coordinating Council. I do not know that we will need a disclaimer here.

Mr. DUGAN. No disclaimer.

Chairman SARBANES. The Council includes the American Bankers Association, the American Council of Life Insurers, the American Insurance Association, and the Securities Industry Association. Mr. Dugan is a partner at Covington & Burling, here in town, and I must note, previously worked here on the Banking Committee staff as Minority General Counsel when Senator Garn was a Member of the Committee.

We are very pleased to hear from you, Mr. Dugan.

**STATEMENT OF JOHN C. DUGAN
PARTNER, COVINGTON & BURLING
ON BEHALF OF THE
FINANCIAL SERVICES COORDINATING COUNCIL**

Mr. DUGAN. Thank you, Mr. Chairman, and Members of this Committee. It is a pleasure to be back here today.

As you said, I represent the Financial Services Coordinating Council, and this organization represents thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America. I have represented the FSCC on financial privacy issues since the organization was formed in late 1999.

Every commercial privacy law strikes a balance between protecting the privacy interests of consumers and preserving the clear consumer benefits that arise from the free flow of information in the economy. While consumers expect limits on the disclosure of

their information, they also expect companies to provide them with benefits that can only be obtained through information-sharing. For example, a long-time depositor in a bank wants and expects to receive a discount on a mortgage loan offered by a related mortgage company affiliate, and such "relationship discounts" can only be provided through information-sharing. Privacy laws try to balance these competing consumer expectations.

In terms of financial privacy, we believe that Congress struck the right balance in the Gramm-Leach-Bliley Act. Financial institution consumers now must be provided notice of practices regarding information collection and disclosure, opt-out choice regarding sharing of information with nonaffiliated third parties, security in the form of mandatory policies, procedures, and controls, and enforcement of privacy protections via the financial regulatory agencies.

By any measure compared to 3 years ago, consumers have much more meaningful information, choice, and security regarding their financial information.

At the same time, the GLB Act appropriately allows financial institutions to share information for a variety of plainly legitimate purposes without consumer consent, for example, to carry out transactions requested by the consumer, to deter and detect fraud, to respond to regulators and judicial process, et cetera.

The FSCC also continues to support Congress' decision to treat information-sharing by affiliates in the same manner as sharing within a single institution. In both cases, the opt-out requirement does not apply, as has already been stated. We think this decision reflected the fact that consumers are unlikely to distinguish between, for example, a community bank and its affiliated mortgage lending company. Instead, consumers expect that both affiliates are part of the same community banking organization where information is shared.

Finally, we also continue to believe that Congress appropriately chose to provide consumers with the right to opt-out of information-sharing with third-party commercial companies.

But Congress also rightly chose to reject an opt-in approach, which deprives consumers of benefits from information-sharing, as Professor Cate just described. Consumers rarely exercise opt-in consent of any kind, even those consumers who would want to receive the benefits of information-sharing if they knew about them. In essence, an opt-in creates a default rule that stops the free flow of information, and that makes financial services more expensive and inefficient. In contrast, an opt-out gives privacy-sensitive consumers just as much choice as opt-in, but without the default rule that denies consumer benefits.

In terms of implementation, the Gramm-Leach-Bliley privacy provisions were enacted in 1999 and implementing regulations became effective just over a year ago. While tremendous progress has been made, this is still very much a work in progress.

Nevertheless, the financial institutions and their regulators have received a minuscule number of customer complaints about the privacy provisions. For example, in response to a recent Freedom of Information Act request, the Federal Reserve reported that it had received only 25 privacy-related complaints out of the 4,503 complaints in total that it received in 2001, or .0056 percent of the

total, with similarly low numbers reported by all the other Federal bank regulators.

Having said that, the FSCC recognizes that privacy notices constitute one area in which improvements can and should be made. This is by no means as easy as it sounds, however, because the notice requirements of the Gramm-Leach-Bliley Act are, in fact, quite detailed, as we just heard. The financial institution regulators tried very hard when they issued their regulations to simplify, including through the use of sample clauses, and they told institutions that a notice complying with the GLB Act could fit on a six-page, tri-fold brochure. In their first notices, financial institutions generally took this approach. But a six-page notice is not short, and terms from the sample clauses such as “nonaffiliated third-party” and the other terms that were quoted earlier this morning are the types of legalese that have been sharply criticized.

To address these concerns, many institutions have tried to simplify the language used in their next round of notices. In addition, both financial institutions and their regulators are exploring a simplified, short-form version of the notice that would supplement, but not replace, the longer legal notice required by the Gramm-Leach-Bliley Act. The basic idea is to use simplified terms, be much less legalistic than the longer notice, keep the length to one page, and use common language to make it easier for consumers to compare policies.

The FSCC is leading one of the short-form notice projects in which we have hired a well-known language expert, and we have nearly completed the initial drafting phase.

Let me now turn to the misunderstanding about the amount of State legislative action that has occurred since passage of Gramm-Leach-Bliley.

During this period, no State legislature has adopted a comprehensive financial privacy statute that has exceeded the obligations of the Gramm-Leach-Bliley Act. Nearly 40 States did consider such privacy legislation in 2000, the year after the law passed, but no such statute was enacted. About half that number revisited the issue in 2001, again without final action. And this year, only California has come close to enacting a new law. But for the third time in 3 years, the legislature has chosen not to do so.

We recognize the initiative in North Dakota which we will hear about and the action by regulators, but not legislatures, in New Mexico and Vermont. But taken together, these few actions simply do not constitute a groundswell of State action.

The FSCC believes the States’ diminished focus is due largely to an increased understanding that the Gramm-Leach-Bliley protections are real and need some time to work, and that it is more complicated than it first seems to impose new restrictions without causing major unintended consequences.

In terms of new Federal privacy legislation, we believe that any action that Congress considers should be targeted to specific harms rather than take the form of sweeping data protection restrictions. For example, if the harm to consumers that people care about most is identify theft or excessive telemarketing, then legislation should remedy these problems specifically and not impose broad restric-

tions on information-sharing. The FSCC stands ready to work with public policymakers to address specific consumer harms.

Let me emphasize, however, that the FSCC could not support any new financial privacy legislation that did not include Federal preemption to ensure a uniform national privacy standard. The FSCC also supports extending the FCRA provision that preempts State restrictions on affiliate-sharing, which would otherwise sunset by the end of 2003.

Thank you. I would be happy to answer any questions.

Chairman SARBANES. Thank you, Mr. Dugan, for your testimony. We are pleased to have you back again with the Committee.

Mr. DUGAN. Thank you again, Senator.

Chairman SARBANES. We are now going to hear from Attorney General Mike Hatch, who has been the Attorney General of the State of Minnesota since 1998. He previously served in the 1980's as Minnesota's Commissioner of Commerce, the primary regulator, as I understand it, of banks, insurance companies, securities, and real estate firms doing business in Minnesota.

Attorney General Hatch, we are pleased to have you with us.

**STATEMENT OF MIKE HATCH
ATTORNEY GENERAL, THE STATE OF MINNESOTA**

Mr. HATCH. Thank you, Mr. Chairman. And I want to thank all of you for your leadership on this issue.

I had the opportunity a couple of years ago to watch a hearing in the Minnesota legislature on the issue of privacy. *The Wall Street Journal* had covered it and pointed out that there were 58 lobbyists retained by a variety of different members of the financial industry, the telephone industry, HMO's, insurers, you name it. And they all piled in, and the pressure was immense. Both parties collapsed. They just caved in.

I know that the pressure on you people is immense. I applaud you for your leadership and for your efforts here. It takes guts and courage and it is very refreshing to see that type of leadership in this country.

So, I thank you very much.

The question was raised about, gee, we have gotten all these notices. Why don't people understand them?

I just want to point out, the first letter I received—

Chairman SARBANES. I think if he could bring it right up here next to the table.

Senator SHELBY. Bring it up inside.

Chairman SARBANES. Yes.

Senator SHELBY. That would help.

Chairman SARBANES. Come right on around.

Senator SHELBY. Up near the Senator.

Chairman SARBANES. Don't block—we want Senator Stabenow to see this easel, too.

Yes, that is it.

Senator SHELBY. Okay.

Chairman SARBANES. Now if we put the things on. Good.

Senator SHELBY. That is better.

Chairman SARBANES. Are you okay, Debbie, with that?

Senator STABENOW. I can see it better than you.

[Laughter.]

Chairman **SARBANES**. All right. The panel's okay. So go ahead.

Mr. **HATCH**. Mr. Chairman, Members of the Committee, the point was raised by the financial industry here that, we have all these notices out there. People do need to understand what is going on.

So what is the beef?

All of these notices were sent to me from a former Congressman, Alec Olson, from the 1970's. He is now, I am guessing, 75 to 80 years of age. He says, "What is all this garbage? I don't understand it." Now if a retired Congressman doesn't understand it, how do we expect that two-thirds of our senior citizens who are the subjects of the rip-off that occurs because of this financial fraud, which is targeted to seniors, how do we expect them to be able to discern these issues?

We heard the Attorney General from Vermont read that disclosure statement, and in the end, what they did not say is, listen, regardless of what you do, we are going to share this with our affiliated institutions and we are going to use it in other ways as well. Even if you did read it and understand it, you would have to be a Wall Street lawyer to figure that out.

Here is a letter that I got a kick out of it because it was after Gramm-Leach-Bliley. This lady had gotten a notice from General Motors Corporation and she says: "What is this business about an opt-out? Why do I have to notify them? And I have been in the financial industries for almost 20 years. I find this unacceptable and a bit unbelievable."

Now what is significant, if you notice her name, she is from a leading investment bank in this country and she is in charge of their education. Look at her business card at the bottom. She did not know. And she thought it was unbelievable. Now if she doesn't know, and she is in charge of educating the members of that investment bank, how does that senior citizen know?

Now if we go to the next exhibit, we will try to figure out, how do they know?

This is actually before GLB. But let me assure you, the complaints in our office, we run a consumer division, the complaint load is higher than it was in the past. I do not attribute it to being higher because of GLB. I attribute it just that there is more increased abuse that goes on in a tighter—when employment gets a little rough, the economy gets cool, fraud tends to go up. It's the same thing. It hasn't changed.

Two-thirds, again, still being targeted on seniors.

This one is a Mr. Clinton—I do not know how to pronounce the last name—Sjosten, I guess. It is a Legal Aid lawyer writing this letter. He says that Mr. Clinton is 87 years old. He had a career as a janitor of a church. And he retired. He has been in a nursing home for 10 years. Telemarketers got that information from Montgomery Wards. They charged up \$2,400 on him, an auto club membership. But he doesn't own a car. He hasn't had one for 10 years. A homeowner's warranty plan. But he doesn't own a home. He is in a nursing home. A dental plan. But he has no teeth.

[Laughter.]

Charged \$2,400. And you ask, how can this be? How can we be so inhumane to our senior citizens that we allow this type of ma-

nipulation to go on? That is all he asks. I represented banks in private practice. I was a banking commissioner. Rural banks do not trade this information. They want it kept private. In our State, we have laws. I have represented companies. We have very strong common law, and I think it exists throughout the country, that says, listen, when you come into a bank with your business plan, if I am a business and I come in there with a business plan to get a loan, that bank cannot share it.

Before Glass-Steagall in the 1920's, they would go out and distribute it. They would give it to their investment arm and then they would go steal the business, the idea, the trade secret, if you will, from the client. Well, that was shut down. The law is pretty clear. And banks know, you keep that confidential.

But you know what? Under this GLB, you hear those notices that were read by the Attorney General? It said, your loan data is not public. With whom? What about the checks I write out as a business? What about the checks I receive? That is my customer list. That is a property right, for crying out loud. It is not only a liberty right, but also a property right.

Somebody says, well, jeez, they won't respond in an opt-in. Yes, they will. Pay them.

The financial banks—the people who are selling this stuff, our data, we are on about 300 lists each. This data is being traded around all over the place. And they sell it. They make money on it. Over 300 bucks a year, on average.

Why don't they pay us a little royalty. You know how to get me to go sell my name? Give me some frequent flier miles, maybe I will do it. I do not know. Maybe some people will. But pay them. Don't hog it all for yourself.

If it is a property right, why do we allow them to get away with it on an opt-out? Pay, and people will intelligently make a decision as to whether this property right will be given up.

Do you know what will happen? Information will still flow. There will be companies that will sprout up that will engage in this. That is fine. That is called free enterprise. Why are we against that?

Property rights. What about the personal liberty right? I go out and I give speeches and I ask them, please raise your hand if you have ever had a yeast infection, a hemorrhoid problem, filed for bankruptcy, bounced a check, had a mental illness, gone in for chemical dependency. I go through the whole routine. Please raise your hand. And there is a gasp.

If you look at HIPPA, HIPPA is no better than GLB in terms of the opt-outs. Oh, we are going to have medical privacy. But then there is a little exemption that says, for telemarketing purposes, you are allowed to use it. Well, the exemption swallows the rule.

All of this information is being traded. What about our right to define who we are? Thank God we did not have that type of information going when I was in my 20's. I wouldn't be sitting here at this table.

[Laughter.]

When you are in your 20's, you experiment with ideas, right? And thoughts. Your telephone company can sell the telephone numbers you have.

What about search warrants?

I, as a public official, cannot go pull your bank data without a search warrant without some probable cause because you have a reasonable expectation of privacy, right?

Now, with these laws basically saying, you do not have a reasonable expectation of privacy, guaranteed there will be a day where a judge will say, because everybody else in the world can get this data, why can't the Government, too, without the search warrant?

There is a very strong, compelling issue that is afoot here and it is not the bank's data. It is my data. That is the way it is in Europe. That is the way it is in other cultures. Most people think it is that way here. It is a reasonable expectation of why not—in most contracts we have in America, there is an offer and an acceptance. Where is the acceptance on an opt-out, to give up my private information? Why not just pay me for it? You would be amazed how many people will respond to a little money. That is okay.

Now these are very important rights. It is a personal right. It is a property right. I applaud you for your courage in standing up on this issue and I wish you the best in getting a bill through.

Thank you.

Chairman **SARBANES**. Thank you, Attorney General Hatch.

We will now hear from Representative Jim Kasper, a Member of the North Dakota House of Representatives, who is very deeply involved in the referendum held earlier this year in North Dakota.

As I understand it, I am sure that Representative Kasper will develop this, a statute had been passed that reduced the existing privacy rights under North Dakota law. It was taken to referendum by the citizens of North Dakota and overwhelmingly, the referendum was overwhelmingly passed, thereby negating the statute.

Representative Kasper, we would be happy to hear from you.

**STATEMENT OF JAMES M. KASPER
MEMBER, HOUSE OF REPRESENTATIVES
THE STATE OF NORTH DAKOTA**

Mr. **KASPER**. Thank you, Chairman Sarbanes, and Members of the Committee.

I want to comment before I start my testimony how much I agree with the three distinguished Senators and your opening remarks. You are right on. And the people of the United States are right on with you, as we found in North Dakota.

I am a first-term representative in North Dakota. We have a part-time legislature in our State. We meet for 3 months every other year and then we go back to the real world of business.

My background has been the insurance and financial securities business for my whole career. I even started that career in college as a senior to help support my newly gotten wife, who has been with me the 30-some years that we have been out of college.

Little did I know when I came to the legislature of North Dakota that the bulk of my time in that freshman term would be spent battling the banks on the issue of privacy. But that is exactly what happened.

North Dakota had a privacy law that was developed and enacted in 1985 at the bequest of the banks, and it allowed no affiliate and no nonaffiliate sharing of information. So private information was totally private. In 1997, our law was amended quietly at the re-

quest of the banks to allow affiliate-sharing, probably in anticipation of Gramm-Leach-Bliley. So, we had that item in North Dakota law. We also had the bank loopholes, so to speak, in North Dakota law where banks marketed and continue to market insurance in small towns.

I have competed with the financial services of the banking industry my whole career in North Dakota. So, I have an idea of what they do, how they compete, and what their strategies are.

It is my understanding that the banking industry is being led in their battle to defeat privacy laws like North Dakota by the organization that is represented here today and by, I think, a financial roundtable organization, are the groups that—there is a focused effort, in my opinion, to stop the privacy laws from changing. And that is what happened in North Dakota.

The banking industry had their bank law introduced into our State Senate, Senate bill 2191. That, in essence, repealed North Dakota banking law and adopted the Gramm-Leach-Bliley definitions of privacy.

I want to share with the Committee and read what their arguments were, why the North Dakota legislature should pass their law and throw out our very protective privacy law. Here is what they said: “North Dakota needs to pass Senate bill 2191 to adopt Gramm-Leach-Bliley in North Dakota law so that we will be in compliance with Gramm-Leach-Bliley.”

This Committee knows that that is a joke. They knew that that was a joke, but that was one of their strategies—confusion.

“North Dakota will experience job loss if we do not pass Senate bill 2191.” Now, you tell me how we are going to lose jobs, but their idea was the bank calling centers will pull out of North Dakota if you do not pass 2191. “North Dakota will experience negative economic development if we do not pass Senate bill 2191.” Businesses will not come to North Dakota because it will be too onerous to comply with old North Dakota privacy law.

There is no cost at all to comply with North Dakota privacy law. The businesses go on doing what they do and their information is protected because one thing in North Dakota law, not only do we protect consumer privacy, but we also protect all privacy.

So business transactions, ag transactions, nonprofit transactions are all private.

“We do not want North Dakota to be the only State in the Nation, an island, which has different privacy laws from other States.” Obviously, as the Attorney General from Vermont stated, there are other States that have privacy laws like North Dakota. And as the legislators of the various States begin to realize what GLB privacy is all about, we are going to see more State legislators introduce laws. I know of two States right now that are contemplating, legislators who are contemplating initiating privacy protection laws like North Dakota’s in their legislature in their next session.

The most funny of all, “If we do not pass Senate bill 2191, the people of North Dakota may not be able to use their ATM’s, credit cards, and their checking accounts.”

In a recent trip to California, at the invitation of Senator Jackie Speier to work with the California assembly, most of the goal was to try to convince some Republicans to support Senator Speier’s bill

because that has become a partisan issue, which it should not be. These were their same arguments.

So this is a national strategy that I submit is being utilized and orchestrated by the banking industry to stop privacy laws from being passed and to try to repeal a North Dakota law.

Anyway, these arguments convinced my colleagues in both the House and the Senate to overwhelmingly, with between a 70 and 80 percent vote, pass their bill. There were just a handful of us who attempted to stop that bill. Two of us were freshmen legislators, and you know how much credibility freshmen have any place. So the bill was passed. The law was signed by our governor, who was a former banker, and it was enacted into North Dakota law.

Fortunately, that is not the end of the story because a group of citizens called Protect Our Privacy formed. Volunteers. No money. No budget. Just a goal to repeal Senate bill 2191 in North Dakota. And in the course of a few short weeks, gathered the number of signatures necessary, a little over 17,000, to repeal the law, or to refer it and put it to a vote to the people.

When you consider that we only have 640,000 people, 17,000 is a big number. It is equivalent to almost 900,000 signatures in the State of California.

Their initiative is going forward, as this Committee heard. And by the way, I predict that when and if their initiative is on the ballot, it will be on the ballot, unless the California legislature acts responsibly next year, that initiative is going to overwhelmingly succeed.

The more money the big banks spend, the more the people get angry, and that is exactly what happened in North Dakota. The banks were well financed. Their first campaign statement showed they had \$129,000 raised. We had \$2,800. By the time the whole battle was done, their media blitz throughout the State of North Dakota was enormous. They attempted to persuade the people of our State that all the arguments which I shared with you earlier were needed to keep the bill.

Our statement and position was very simple. Whose information is it, anyway? Do you own it? Should you have the right to control it? Or should the banks own it once they get it and be able to share it and sell it without your consent and knowledge? That was the focus. That is all we could talk about because that is the truth and the bottom line of this privacy battle—whose information should it be, as Attorney General Hatch has indicated?

When the people understood, the vote was 73 percent to throw out the Senate bill 2191 and go back to North Dakota law. I submit that as more and more people in the United States become aware of what this is all about, you are going to see more and more State legislators move forward to do the same thing in their State.

Unfortunately, that is time-consuming and costly and you have the might of the big banks, who will be there to try to thwart the issue every time it comes up in every State legislature. We had full-time lobbyists up there from the banking industry, three or four of them. The credit union lobbyists were involved. The big banks came in. The local bankers came in to talk to their legislators and the legislators were, frankly, somewhat misled and confused on this issue because they talk real good. But the people

know better and the people of our country want their private information protected.

If we do not do this, if we do not move forward with protection, because the lifeblood of this battle for financial services is the free-flowing of consumer confidential financial information, Gramm-Leach-Bliley does not foster competition. It eliminates competition.

As a small business person in the financial services industry, I have a very difficult time competing with the Wells Fargos of the area. When a person comes in to get a loan and provides their tax return, their financial statement, their history, and the loan officer just goes to the insurance agent or the securities agent and says, here, here's some stuff. Look it over. Go call this guy.

That happened on one occasion with my best client in Fargo, who I have served with life insurance for 20-some years. An insurance agent from Wells Fargo called on them and had all of their financial information and, in fact, showed them a sophisticated insurance proposal where they had to have gathered their incomes, their date of birth, et cetera. My client knew nothing of it, had never met the agent before, and this guy comes in and shows him the information. He called me. We looked at it. We threw it in the garbage. But the point is, why should that insurance agent have gotten that information in the first place? He shouldn't have.

My mother in Beulah, my hometown, western North Dakota, just had a CD come due. The bank teller recommended that she put it into an annuity. The bank teller knows nothing about my mother's financial information and her background and her financial needs.

My mother, thank goodness, said, I call my son on these things. [Laughter.]

She did. And we are looking at what she should do with her CD.

The point is, people are handling confidential information all over the place. It has run amok. And I hope that this Committee will have the courage to stand up to the tremendous lobbying effort you are going to see and reverse the things in Gramm-Leach-Bliley that need to be reversed, such as no sharing of information to nonaffiliates, period. A no-opt.

An opt-in sharing of information for affiliates. And the joint marketing agreement loophole, that needs to be fixed. I understand why it was introduced, to allow the small banks and credit unions to compete with the Wells Fargos of the world. That definitely needs to be fixed.

Mr. Chairman, and Members of the Committee, I see my time is up. I have a lot more I could say about this issue. But I thank you very much for the opportunity to be here.

Chairman SARBANES. We thank you very much, Representative Kasper. It is a very instructive story that you tell and we really appreciate it.

Before she leaves, I do want to add just one dissent to what you said. You said that the freshmen members of the legislature do not have much influence.

[Laughter.]

I agree with that statement generally. But I do want to underscore what a tremendous exception to that statement our freshman Member, Senator Stabenow, has been here, both in the Committee and in the Senate.

Senator STABENOW. Thank you.

Chairman SARBANES. We will now turn to Phyllis Schlafly. We are very pleased that you are here with us today. As we all know, Phyllis Schlafly is the President of the Eagle Forum. She has been an outspoken advocate on a number of very important issues and has testified frequently here in Congress. She is the author/editor of numerous books and publications. Ms. Schlafly, we are delighted to have you with us today.

**STATEMENT OF PHYLLIS SCHLAFLY
PRESIDENT, EAGLE FORUM**

Ms. SCHLAFLY. Thank you, Mr. Chairman, and Senator Shelby.

Totalitarian governments keep their subjects under constant surveillance by requiring that everyone carry “papers” that must be presented to any Government functionary on demand. This is an internal passport that everyone had to show to authorities for permission to travel within the country, to move to another city, or to apply for a new job.

Having to show papers to Government functionaries was bad enough when papers meant merely what was on a piece of paper. In the computer era, personal information stored in databases can be used to determine your right to board a plane, drive a car, get a job, enter a hospital emergency room, start school, open a bank account, buy a gun, or access Government benefits such as Social Security, Medicare, or Medicaid.

While each classification currently has its own set of rules, connecting all these dots would amount to the personal surveillance and monitoring that are the indicia of a police state. The Washington buzz words, “information-sharing,” are often put forth as the solution to 21st Century problems, but this has significant privacy implications that I am very happy you are addressing.

The global economy is obsessed with gathering information. The lifestyle or profile of each consumer is a valuable commercial commodity. The checks you write and receive, the invoices you pay, and the investments you make reveal as much about you as a personal diary. Where I shop, how often I travel, when I visit my doctor, how I save for retirement are all actions known to financial institutions, which connect the dots of my life and create a valuable personal profile. This compilation of personal information is bad enough, but the sharing of it without my consent is even worse.

True privacy protections encompass the principles of notice, access, correction, consent, preemption, and limiting data collection to the minimum necessary.

The bill commonly known as Gramm-Leach-Bliley had the financial goal of streamlining financial services, thereby increasing affiliation and cross-company marketing. But it was conflicted with the goal of true financial privacy. Greater affiliation meant greater information-sharing. Interjecting the right of individuals to control their personal information into that streamlining equation was perceived as a threat to this big business scheme.

Gramm-Leach-Bliley does not provide consumers with any opportunity to decide for themselves about the transfer of their private information among affiliates. Particularly troubling is the large number of companies marked as affiliates. For example, the Bank

of America has nearly 1,500 corporate affiliates, and Citigroup has over 2,700. There is no opportunity to stop this free flow of personal information.

Gramm-Leach-Bliley did include a privacy notice provision. Privacy notices should be simple documents outlining what kinds of information are collected and how the business plans to use that information. However, the notices sent to consumers as a result of Gramm-Leach-Bliley turned out to be too complicated for the public to cope with and they were always written in very fine print.

Gramm-Leach-Bliley provided the right to opt-out of information-sharing but only to third parties. Figuring out how to prevent the sale of your personal financial diary, and to whom you were actually denying it, was made very difficult. Real opt-out consent depends on being able to understand what you are saying no to.

In 1998, the Clinton Administration proposed a Federal regulation called Know Your Customer, which would have turned your friendly local banker into a snoop reporting to the Federal database called FinCEN any deviation from what the bank decided is your deposits/withdrawal profile. The American people and the Eagle Forum was a part of this effort, responded with 300,000 angry e-mail criticisms and the regulation was withdrawn. The department subsequently said they would no longer receive e-mail criticisms. However, the Bank Secrecy Act still requires banks to share some personal information with the Government through suspicious activity reports.

The Bush Administration's proposed regulations to implement the USA PATRIOT Act's Anti-Money Laundering provisions are even more intrusion than Know Your Customer. *The Wall Street Journal* reported that the Treasury Department entered into an agreement with the Social Security Administration to access a database to verify the authenticity of Social Security numbers provided by customers at account opening.

Congress promised us that the Social Security number would never be used for anything else when it was created, and certainly not for identification purposes. Giving financial institutions access to Social Security Administration's database contemplates using the number as a national ID number, which is a step in the wrong direction.

I remember after President Nixon opened up China, *The New York Times* printed a large picture of a warehouse of what were called dangens. This was a manila folder containing all the personal information on every person in China. It started in school. It followed them all through life, with all of their job information.

It is the computer that makes it possible to create a dangen on every American citizen, and that is not America.

In conclusion, neither Government nor private business should act as if they can own, share, display, or traffic our personal information. It is a property right issue. Our personal financial data should be protected by a firewall and accessible only to those to whom the individual gives the authority.

Thank you very much, Mr. Chairman.

Chairman SARBANES. Thank you very much, Ms. Schlafly. We are very pleased to have you here today.

Our concluding panelist is Ed Mierzwinski, who is the Consumer Program Director of the U.S. Public Interest Research Group. He comes today testifying on behalf of a number of consumer groups, both the broader groups—Consumer Action, Consumer Federation, Consumer Union, and then a number of groups that are more specifically focused on the privacy issue—the Electronic Privacy Information Center, Identity Theft Resource Center, Privacy Rights Clearinghouse, and Private Citizen.

We are very pleased to have you here, sir.

**STATEMENT OF EDMUND MIERZWINSKI
CONSUMER PROGRAM DIRECTOR
U.S. PUBLIC INTEREST RESEARCH GROUP
ON BEHALF OF:**

**CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA
CONSUMER TASK FORCE ON AUTOMOTIVE ISSUES
CONSUMERS UNION, ELECTRONIC PRIVACY INFORMATION CENTER
IDENTITY THEFT RESOURCE CENTER, JUNKBUSTERS, INC.
PRIVACY RIGHTS CLEARINGHOUSE, PRIVATE CITIZEN, INC., AND
U.S. PUBLIC INTEREST RESEARCH GROUP**

Mr. MIERZWINSKI. Thank you, Mr. Chairman and Members of the Committee, and in particular, I will recognize Senator Shelby, the founding Co-Chair of the bipartisan Congressional Privacy Caucus, for his leadership, as well as yours.

The organizations that I am representing today believe strongly that people have a strong right to privacy and that privacy should be based on Fair Information Practices.

Recognizing when it enacted the Gramm-Leach-Bliley Act, that it was increasing the potential for privacy invasions, Congress acted by establishing Title V to try to protect privacy. The basis of Title V we believe is flawed and a lot of that has already been articulated by some of the other witnesses on the pro-privacy side today.

The primary basis of the Act is that it is based on notice. Notice is not enough. As we have seen from the first 2 years of examples, the notices are unclear, the notices are indecipherable, the notices are unreadable.

The Privacy Rights Clearinghouse commissioned a consultant, Mark Hochhauser, on readability in 2001. He surveyed 60 of these notices and found that they were written essentially for a graduate school education.

The average consumer has not been to graduate school. And I concur with General Sorrell that there should be something like a nutrition notice at the front of every privacy notice and the check-off box for voting out or voting in, whether it is an opt-out or an opt-in, and of course, we would prefer an opt-in, as I will discuss briefly. That check-out box should be on the front page, not on the 8th page of a 6-point type document with 27 to 35 word compound sentences.

This year, as part of California PIRG's efforts to enact the Jackie Speier legislation, SB-773, broad consensus legislation supported by a number of privacy and consumer organizations in the State of California, California PIRG updated the Hochhauser study with a study of 10 privacy notices in August. We found that the best of the 10 got a C minus. So notice is not enough.

In my testimony, I also refer to a very disturbing decision by a U.S. District Court Judge in California in an unrelated financial privacy case, but a related case to notice provisions. In that decision, Judge Zimmerman suggests that a large telephone company may have hired consultants that taught it to purposely make its privacy notices deceptive. And I cite some of those notices. How to convince people not to opt-out. How to convince people that the notice is a nonevent.

There were a series of consultants actually hired by the company to teach the company how to make its notices unreadable, essentially. So, I am very concerned about that. And that is, of course, one of the reasons that we think notice is not enough.

The second problem we have with the bill, of course, is that the consent provision in the bill only applies to some transactions. It applies, not to all third parties. It applies to some third parties.

Let's be very clear. It is an opt-out, meaning that you have to affirmatively say no, and it does not apply to all transactions. It only applies to some third parties, essentially limited to telemarketers.

Transactions between and among affiliates and joint marketing partners—and there is no exception in the law that prevents large institutions, some of them have as many as 2,761 affiliates, as we heard earlier, that prevents large institutions from also using outside joint marketing partners as well.

So the fact is the bill is based on only part of the Fair Information Practices, which we believe the data-collectors should subscribe to.

In recognition of the fact that there had been a major privacy scandal that had been discovered by the State of Minnesota Attorney General, Attorney General Hatch, and his office, the U.S. Bank case, the Congress included an encryption provision in Title V to try to tighten it up a little bit more. The encryption provision was included and it stated that telemarketers could not obtain the credit card numbers of consumers.

The reason for that was that in the U.S. Bank case, as Attorney General Hatch has described, the consumer never gave out their credit card number to telemarketers. Their bank gave their credit card number to telemarketers.

As the Attorney General has testified, and as General Sorrell has testified as well, the encryption provision has not worked.

Essentially, Gramm-Leach-Bliley codified the preacquired account telemarketing programs that are in place at many of the largest banks in the country. These banks are no longer providing the credit card number directly to the telemarketer, but the telemarketer has a button that he or she pushes that allows the bank to bill the consumer.

Now one of the witnesses testified that opt-out doesn't work and that opt-in would work even worse.

In Attorney General Hatch's recent settlement with Fleet Bank, he sent a letter to the consumers who had been victimized—excuse me—Fleet Mortgage Company, an affiliate of Fleet Bank. You would think that this kind of tawdry telemarketing would be limited only to credit card companies, but mortgage companies are doing it, too.

Attorney General Hatch sent a letter to a number of Minnesota consumers asking them whether they wanted to opt-in to his settlement and get their money back. Well, 50 percent of them responded within 2 weeks.

If you write your opt-in letter well, and if you offer people something, opt-in does work. And if you are trying to get people's money back from a rip-off telemarketer who is in league with your bank, opt-in does work.

So, we were very pleased to see that.

The last point I want to make, of course, is that the best part of the Gramm-Leach-Bliley bill is, in fact, its States rights fail-safe, the so-called Sarbanes Amendment, that has allowed the States to experiment. As the great Justice Louis Brandeis said, "The States are the laboratories of democracy." And although the industry has sent hundreds of lobbyists out to Fargo, out to Sacramento, out to Bradelborough, I have been to all these places, I have seen all the industry lobbyists, Montpelier, excuse me, in Vermont, and all the other State capitals where the State PIRG lobbyists work, the industry is trying to stop these laws, but these laws are being considered and you need to protect the right of the States to continue to try to pass stronger privacy laws.

The costs of privacy have been articulated by industry as tremendous—billions and billions of notices, the loss of the free flow of information.

I want to point out that there are costs to the lack of privacy as well. I would like to enter into the record a study* by independent consultant Robert Gellman which refutes a number of the industry-funded studies that the industry relies on to make its points.

The fact is the lack of adherence to Fair Information Practices leads to identity theft, which costs hundreds of thousands of consumers, hundreds of dollars a year in out-of-pocket costs, hundreds of hours in trying to clear their good names, extra costs because their credit reports are in error and they must pay extra for sub-prime credit, the costs of profiling, the cost of being targeted and the cost of being put into a box that you are a Tobacco Road consumer and not a Gucci Gulch consumer on one of these 300 lists, and you pay too much for credit and you only get offered mediocre offers. These costs are very substantial and these costs affect consumers in a very negative way.

In terms of the free flow of information, industry wants to have that one both ways. Many banks are limiting their flow of information about a consumer's good credit in order to prevent that consumer from having a good credit report and a good credit score.

They are gaming the credit-scoring system and Comptroller Hawke did a speech on this several years ago, and he was very concerned about it. If a consumer's credit score is affected by a limit on how much information banks share with credit bureaus, that consumer doesn't get any offers. That consumer doesn't get any opportunities.

So there are some very serious costs to a lack of privacy and identify theft is one. Profiling is another. The cost of paying too much for credit because banks are gaming the system is another.

*Held in Committee files.

Stalking is even a problem of the costs of lack of privacy, as the case of Amy Boyer several years ago.

I want to conclude briefly by saying that the State PIRG's and the other consumer and privacy groups that are signed on to our testimony today very much appreciate that you held this hearing. We will continue to work in the States on privacy, financial privacy issues, identity theft issues, credit-scoring reform, and other aspects of financial privacy.

We are disappointed that some industry groups have tried to suggest that financial privacy prevents them from helping Director Ridge from fighting the terrorists as one of the excuses they make to try to roll back the State privacy laws.

We are disappointed also that they say you won't be able to use your ATM card if we pass strong financial privacy laws. But that is life in the big city and we will continue to fight and we appreciate you fighting with us.

Thank you very much.

Chairman **SARBANES**. Thank you all very much. This has been a very, very helpful panel.

We have been joined since the panel began by two of our colleagues and I am going to turn to them now to see if they want to make an opening statement before we start directing questions to the panel.

Senator Akaka.

COMMENTS OF SENATOR DANIEL K. AKAKA

Senator **AKAKA**. Thank you very much, Mr. Chairman.

It is good to hear witnesses from around the country on the issue of financial privacy.

The sharing of consumers' financial information needs to be regulated to reduce frustrations and the likelihood of the misuse of that information. Financial institutions are required to provide their customers with information regarding their privacy policies on an annual basis. Financial institutions are prohibited from sharing nonpublic personally identifiable customer information with non-affiliated third parties, unless customers are provided with an opportunity to opt-out.

My constituents in Hawaii have contacted me to express their frustrations with the opt-out process. The opt-out process is time-consuming for many individuals and in some cases, privacy notices are too difficult to understand. I agree that the notices are not enough and are difficult to understand.

Financial privacy is one of many areas in which consumers' financial literacy needs to be increased. Consumers need to be fully aware of their opportunities to exercise financial privacy restrictions and how to do so.

In addition to education, a complete examination of the current laws intended to protect personal financial information is needed to ensure that consumers are protected.

Again, Mr. Chairman, I thank you for conducting this hearing.

Chairman **SARBANES**. Thank you, Senator Akaka.

Senator Corzine.

COMMENTS OF SENATOR JON S. CORZINE

Senator CORZINE. Thank you, Mr. Chairman.

I can only tell you that there is almost nothing that Senator Akaka said that I would disagree with or preparing myself for this, knowing the concerns of both the Chairman and Ranking Member with regard to this privacy issue, that I want to very much identify with, needs to be cleaned up.

I hear about this all of the time as I visit with constituents around the State, a growing, growing concern about invasion of one's personal information, the integration of the marketing aspects of information collected by those that have access to financial transactions and so on.

I am anxious to be a consistent and full participant in this process, and I will emphasize this financial literacy issue.

I can tell you that I have read a lot of these statements myself. I usually go to sleep before I get to the end of them, and know where you are supposed to sign off.

[Laughter.]

I think it is a ruse on the public with regard to this opting-out process.

So, I look forward to working with you and the other Members of the Committee in this area.

Chairman SARBANES. Thank you very much, Senator Corzine.

Both Senator Corzine and Senator Akaka have been very, very active on the financial literacy issue and we certainly appreciate their concern.

Professor Cate, I want to ask you a question right off the bat.

The Financial Services Coordinating Council, who Mr. Dugan is representing here, issued a booklet, not too long ago on what they call the drawbacks of an opt-in regime. And you were the author of that booklet. You recall that, I presume.

Dr. CATE. I do. I think it was 2 years ago. But, yes, sir.

Chairman SARBANES. All right. Now in that, you are arguing against the use of opt-in. And I do not want to address the opt-in issue for the moment.

In the argument you make against opt-in, you say: "Lawmakers should resist the mounting pressure to expand the use of opt-in, for eight compelling reasons." And the first reason you give is, "Opt-in and opt-out both give consumers the exact same level of control over how information about them is used. Under either system, it is the customer alone who makes the final and binding determination about data use." Now, of course, we have heard some criticisms about how the opt-out system works. But let me ask you this question. Am I to take from this statement that you support requiring opt-out for the sharing of any financial information?

Dr. CATE. I think that would not be accurate to say that I support opt-out for the sharing of any financial information.

Chairman SARBANES. I see. Well, you make the point here that opt-out gives—under both, the consumer has exactly the same level of control and therefore, you should use it. The alternative to opt-out is opt-in. And then you are very critical of opt-in. But you say, with opt-out, they can control their information. Is that correct?

Dr. CATE. Yes, sir, Mr. Chairman.

Chairman SARBANES. Should we have opt-out at least as a starting point or as a minimum for the sharing of financial information?

Dr. CATE. I would not support that across the board.

Chairman SARBANES. Would not?

Dr. CATE. I would not, sir.

Chairman SARBANES. How does that square with your statement here?

Dr. CATE. It squares in this way. If there are areas or uses of information that the Congress believes that consumers should have control over, I think the opt-out is a better and certainly less expensive system for allowing consumers to exercise that control.

I personally do not believe that under the First Amendment that the Congress has the Constitutional authority to extend to consumers the right to exercise control over all uses of their financial information.

Chairman SARBANES. You do not think the information belongs to the consumer?

Dr. CATE. I think the question of who it belongs to is more or less irrelevant. Under the Constitution, I do not believe Congress has the authority to use the power of the courts or to use regulators to enforce that restraint on the flow of information.

Chairman SARBANES. To opt-out as well as to opt-in?

Dr. CATE. Yes, sir, although I believe the opt-in restraint is more severe, and so the First Amendment impediment would be greater.

Chairman SARBANES. So if I am a consumer and I give this information to a financial institution, it is then gone. They can do what they wish with it?

Dr. CATE. There are many uses of information, which, if they do not present a risk of harm or—many uses of information, most uses of information, which I think in this country we presume—

Chairman SARBANES. Should I make that judgment as the one who provided the information? Or do you get the information from me for a limited specific purpose, and then once you have it, can you then—you being the financial institution—turn around and do with it what you will?

Dr. CATE. Well, Mr. Chairman, I believe it is a matter of law.

If, in fact, information is obtained under an express condition that it will not be used elsewhere I think that restraint should be enforced, as the Federal Trade Commission has repeatedly done online and elsewhere.

But the Constitution I think limits the power of the Government to create an impediment at the start to all uses of financial information or other forms of information, absent some form of substantial or compelling governmental interest.

Chairman SARBANES. That is interesting. What do you think of that, Ms. Schlafly? Do you think that we are precluded from placing some restraint on the use of that information?

Ms. SCHLAFLY. I am amazed.

Chairman SARBANES. I am stunned.

Ms. SCHLAFLY. I think the information about what I do and what I buy is my property. I do not think it belongs to somebody else. If there is anything the United States stands for, it is individual property rights.

Chairman SARBANES. Attorney General Hatch, what is your reaction to that?

Mr. HATCH. Mr. Chairman, there is \$15 to \$20 billion of telemarketing fraud in this country each year. As I said, two-thirds of it is targeted to senior citizens, who I do think we have some responsibility to guard.

We know that most of this is done through what is called pre-acquired accounts, meaning that they have the information from a bank or a credit card company. They never have to ask for that information from the consumer because they already have it. It has already been obtained from the bank.

That is a compelling State interest right there.

I just don't understand. If opt-out and opt-in are the same, why would it make any difference as to which information is being protected? The point you were making, I do not know if we received an answer.

Chairman SARBANES. My concern with this statement is, the argument that is made against opt-in, which would be an up-front permission from the provider of the information, or how it is used, the argument that is made is that the consumer can protect himself because he has opt-out.

Now there is a big difference between the two, but opt-out at least means that if the consumer initiates it, he can then say that I do not want that information provided. The other way, with opt-in, they have to get the permission to begin with.

Professor Cate uses the argument in this pamphlet that you should not have opt-in because you have opt-out. So, I just asked him, well, does he then apply opt-out to all aspects of providing information? I am told, no, he doesn't.

I am now told that, amongst other things, he thinks there is a Constitutional impediment to doing this, which I do not agree with. But, in any event, even as a policy matter—that is our problem.

Here we have—it is a disingenuous argument to say, we do not need opt-in, because they have opt-out.

Then you ask, well, would you apply opt-out to all aspects of the sharing of financial information? Then it is, no, no, we wouldn't do that. So there is our problem.

Yes, ma'am.

Ms. SCHLAFLY. Senator, it seems to me that the difference between opt-in and opt-out is the default. Those of us who use computers know how valuable it is what the computer defaults to when you do not make an affirmative choice.

With opt-in and opt-out, one way the default goes to the bank and the other way it comes to you. I think that that is an extraordinary difference.

Chairman SARBANES. I think that is a very important point and I said at the outset, I wanted to be careful. Because there is a very strong argument that opt-out is not adequate, the one you just made. Therefore, you should have to get an affirmative decision.

But I cannot even get Professor Cate to give me opt-out on the sharing of the financial information. That would be a beginning here. At least we would begin to parse this thing out and see if we could not make some advance.

I am told, no, no.

Well, I have used my time. If my colleagues will indulge me, I want to ask Mr. Dugan one more question.

Mr. Dugan, you cited that these States were trying to pass these statutes now under the fact that under Gramm-Leach-Bliley, it is specifically stated that the States' action in this field, that it is not preempted, that they can move ahead. And so, people go out and they fight these battles out in the State legislatures. As I understand it, you yourself have been in a number of State legislatures on this fight.

Mr. DUGAN. That is correct.

Chairman SARBANES. And you make the point that it has not yet passed, I think you said, in any State legislature. Is that right?

Mr. DUGAN. That is right. Any comprehensive statute.

Chairman SARBANES. I thought you said you drew from that the conclusion that this issue was a fading or a passing issue across the country, and that this was demonstrated that the public doesn't really care about this issue and that it is going to go away. Is that your view?

Mr. DUGAN. I do not think I quite said that. What I was trying to get at—

Chairman SARBANES. You came close to it. But, anyhow.

Mr. DUGAN. What I was trying to get at was this.

Senator SHELBY. You did not say it. You were hoping it.

[Laughter.]

Mr. DUGAN. I think there is a perception, every State or many States in the country, that the trend has been for State legislatures to take this up and pass financial privacy legislation that goes beyond Gramm-Leach-Bliley. And all I was trying to say was, in our experience, the trend has been in the other direction, with the notable exception of California.

Chairman SARBANES. And North Dakota, by direct action of the people rather than the legislature.

Mr. DUGAN. That is right, but that was a restoring of a law that was previously on the books. My point is that the year after Gramm-Leach-Bliley passed, there was a huge set of bills introduced that went way beyond Gramm-Leach-Bliley in many States and debated in many States. None of them passed. Then the second year, it was about half that number. And in the third year, it had dwindled to a relatively few number of States that were doing it.

I am not trying to say that there is no interest in it. There obviously is. There was intense interest in California.

I am just saying that if you take and look at the country as a whole, and what legislatures have done, I think that there has been a repeated set of circumstances in which legislators have decided that it has not been as easy to pass something like this in a way that works that doesn't create unintended consequences.

There is also a notion that this new Federal scheme has gone into effect, and we should give it a chance to work before we decide to layer on inconsistent privacy statutes across the country, which the FSCC thinks would be a disaster.

Chairman SARBANES. So, you think it is going to go away?

Mr. DUGAN. No, I did not say that. I think we have work to do. I think there has been a problem with the notices. They do have to get better.

Chairman SARBANES. Where are you going to be if California passes an initiative on this issue? The California legislature came close this year, as I understand it, very close. But where are you going to be if they pass an initiative in California?

Mr. DUGAN. Senator, that is a hypothetical situation.

Chairman SARBANES. Do you think an initiative would pass in California on the basis of the North Dakota experience?

Mr. DUGAN. I certainly would hope not.

Chairman SARBANES. Mr. Kasper, you wanted to add to that?

Mr. KASPER. Yes, thank you, Mr. Chairman.

Just an observation. If the other States in the last 2 to 3 years were bombarded by the banking lobbyists as North Dakota legislators were, when they were confused and misled by the bank arguments, which I laid out earlier, I can understand why no legislation passed in those other States.

We were different in the fact that we had a law to protect and the people decided to refer it. And when the people made connection with the truth, the people spoke loudly and clearly. That is what I believe is the sentiment all across the United States, as you have heard from your colleagues here on the panel and from the panel members themselves.

This is a national strategy, I believe, by the financial services industry, led by the banking industry, to confuse the issue and kill any type of legislation that is attempted in North Dakota.

I wish they could come to North Dakota now and talk to some of my legislative colleagues who went through this media battle and now understand the issue, who are very angry at the way that our legislators were misled by the lobbying efforts of the banking institutions.

So you confuse. You mislead. Sometimes you out and out lie. And the legislators, with that type of pressure, are going to go along with no change because they may think that is what is in the best interest of their State, which it is not.

Chairman SARBANES. Yes, Attorney General Hatch.

Mr. HATCH. Mr. Chairman, I would like to point out for Minnesota, that at least the lobbying effort that occurred did not diminish the issue. It is coming back and it will continue to come back until something passes.

But I do want to point out, it wasn't just the banks. There is a lot of different interests involved in this. You have the telemarketing companies. You have, as I mentioned, insurers, HMO's.

And frankly, if I took a poll of the banks in Minnesota, you would find probably a majority in favor of privacy, but they would be the smaller ones. They do not want this information out there. They do not want this information being taken by a Citibank or whoever, and then stealing their clients. It is not the small ones who are doing it.

So do not give too bad a rap here to the banks of America. A lot of the small ones are not interested in this issue at all. They have operated very well with an opt-in system because they do not want to do it.

As I mentioned before, a First Amendment right to disseminate, does this mean that an employee of mine—I have companies that represent companies, an employee can take the customer list? They

have a First Amendment right to disseminate it? Does the bank have a right to take the bank deposits of my clients and go disseminate it to their competitors, their customer list? I do not think so.

There has been very strong privacy rights by common law in this country with regard to property assets. I would hope that GLB did not touch that. But you know what? I suppose one could interpret it to have done so. What a tragedy?

Chairman SARBANES. I am going to yield now to Senator Shelby. Did you want to say something?

Mr. DUGAN. Mr. Chairman, I want to respond on the point about smaller banks.

I think the fact is that smaller banks have to share information with other financial institutions to offer the range of competitive products that diversified financial institutions can provide. And we are very strong supporters of that kind of sharing, which is precisely what was recognized in Gramm-Leach-Bliley, and which was precisely what was recognized even in the California bill that almost passed.

Chairman SARBANES. Well, but should the consumer have a say in that? Shouldn't he have a say?

That's all. That's all. I do not think there is any approach that would rule it out absolutely. It would just put the decisionmaking authority in the person who provides the information. It is personal information about them, and they should have, it seems to me, should be able to control where it goes and what is done with it.

But I have strayed over my time. I yield to Senator Shelby.

Senator SHELBY. Thank you, Mr. Chairman. Again, I want to thank you for calling this hearing. I also want to commend Senator Sarbanes, that in the conference, we were all on it with the House, dealing with Gramm-Leach-Bliley, Senator Sarbanes had the foresight to offer the amendment to protect the States' ability to deal in this area over and above.

I think that is so important to Senator Sarbanes. I have been involved with you and I have worked with you and I have worked with a lot of people on this. I believe myself that the people ultimately are going to prevail here. The people are going to win this battle, no matter how much money is spent against it because this is an important right of the people, as Ms. Schlafly talks about.

Mr. Kasper, I have a few observations and some questions.

One, I want to commend you for getting involved and what the people of South Dakota did. That was not isolated—of North Dakota, excuse me. Made a mistake.

Mr. KASPER. That is all right.

Senator SHELBY. But what they did, they understood the issue. And if the people understand the issue, they are not going to give their privacy away. I believe that. Not many of them, and so forth.

I do want to also take a few seconds and commend both the Attorneys General here. They have been outspoken. Somebody has to speak up for the people, and they do this.

Ms. Schlafly, we have worked together on a number of issues, and this privacy issue cuts across all political philosophy, and all parties, Democrats, Republicans, and so forth.

I have worked with Mr. Mierzwinski on a number of occasions.

I wish my State of Alabama had a referendum proposition, a proposition where you could bypass the legislature, if you had so many people. A lot of the States do. And that goes back to the Sarbanes Amendment. That is going to be the linchpin to this, I believe.

Now, I want to direct this to Mr. Dugan and Professor Cate.

I would like to know from you, if you can, to the extent that you can provide the details here, what happens to, and I will just use myself here, my personal information when I open a checking account, get a credit card, and that kind of thing. Just say I were to go down the street here and open up a checking and savings account. What happens to that information? Let me just run down a list of questions.

What information are they required to obtain from me? How does the bank use it? Do they share it? And yes, what do they actually share, and who with? Why do they share it? Well, I think we know that. Who do they share it with? Affiliates? Third parties? Partners in joint marketing agreements? You can create those. That is so easy.

Do they sell it? What effort does the bank or financial institution make to ensure its security? Or how can it be secure once it is gone? What about affiliates and third parties who may gain access to the information? Do they undertake efforts to protect it? Who do they protect it from if they are using it?

All these questions I think need to be answered because people in America, across all party lines, are going to be asking. They are beginning to. And hearings like this help. Can you help me there?

Mr. DUGAN. Well, let me start and there is quite a long list.

Senator SHELBY. Sure.

Mr. DUGAN. If there are other things, we would be happy to furnish it for the record as well. Professor Cate can jump in as well.

Senator SHELBY. Sure.

Mr. DUGAN. I think in the first instance, when information is collected from consumers, there are two kinds of information. The first is information that is used to make a judgment about making a loan to you or underwriting insurance for you. That kind of information is covered by the Fair Credit Reporting Act.

And because that information can be used to make an important decision, it can have a very important effect on the consumer, the restrictions on that information under Federal law are stricter than they otherwise would be. In fact, that kind of information cannot be shared with third parties except under very specific circumstances such as sharing with the credit-reporting agencies. It can only be shared with affiliates subject to an opt-out.

If the information doesn't relate to that kind of information, then the Gramm-Leach-Bliley system kicks in and the information can be shared to carry out things that I think everybody would say it should be shared for. It obviously has to be shared with third parties when you write a check and the check goes through the clearing system to other banks to carry out your transaction. It has to be shared with third parties in order to do the very thing you have asked for. And nobody quibbles with that, and I am sure you do not, either, Senator. But I think you then get to the question of, is it shared for marketing purposes?

I think institutions use it to—they would want to know, for example, if you were a good customer of the bank and you had a large deposit, that would be a customer that they would want to make sure was treated well with respect to other kinds of products. If you were a long-time customer of the bank, that kind of information, they would want to know that.

And so, the information would be shared inside the bank in order to make decisions to cross-market products, and it would be shared with affiliates as necessary if they thought that would be useful to provide products and services to you.

Now, if it gets to third parties, that is where Congress drew the line and said, if it goes to a nonaffiliated third-party, then they have to give you the right to opt-out of that type of sharing.

Senator SHELBY. But you can create an affiliate fast, can't you? You can create a joint marketing agreement so fast.

Mr. DUGAN. We think affiliates—

Senator SHELBY. There are a thousand ways to get around.

Mr. DUGAN. We do not think it is getting around. We think an affiliate is all part of the same organization. If you have Citibank and Citibank Mortgage Lender, that is really the same thing to the consumer. It is all part of one organization.

The line comes when the information is shared outside the commonly controlled organization, particularly to commercial companies or nonfinancial companies. And there, Congress drew the line and said, that is a place where the consumer should have some control and that is where they established the opt-out.

We think that is appropriate.

Senator SHELBY. You used the word scheme earlier. A lot of people believe this was a scheme. That is, the opt-out was a scheme to hijack people's personal information, knowing that with all the trouble and all the notices and not understanding what was going on, that most people wouldn't know the real issue. The notices were meant not to let them know, but to let them throw it away.

Mr. DUGAN. Well—

Senator SHELBY. Whereas—wait a minute—whereas, if you go with the premise that this is your information that you send that belongs to your checking account, your savings account, and all this, and it is your property right, as Ms. Schlafly talks about, which I believe, it belongs to you, and you have a confidential relationship, or should have—most people think they do—with their financial institution.

Gosh, how can you justifying selling that, using that without the permission of the customer, the expressed permission? How can you do it?

I think Attorney General Hatch made a good point.

Mr. DUGAN. From our point of view, I do not believe—

Senator SHELBY. And your point of view is the point of view of the people you represent, right?

Mr. DUGAN. It is the people who have to serve their customers every day, and it is an industry that is built on maintaining the trust of their customers.

Senator SHELBY. This is a way to break it down, isn't it?

Mr. DUGAN. Well, that is where we disagree.

Senator SHELBY. I think that is under attack all over America.

Mr. DUGAN. With all due respect, Senator, we think the information-sharing that goes on helps consumers, helps provide—

Senator SHELBY. How does it help them? I want to hear that.

Mr. DUGAN. I will give you an example.

Let's say you had an opt-in scheme and at the beginning of a customer relationship—from our point of view, many consumers do not either opt-in or opt-out. They are less sensitive to this concern.

If you have an opt-in scheme and they do not opt-in to some information-sharing, they just do not pay attention to it and they do not opt-in, then they do not get to hear about some of the benefits that would otherwise apply. For example, if someone has a deposit with a bank, it is a common practice for the bank to give a discount on a mortgage provided by an affiliated company. Or it may be the case that someone has a high-rate credit card loan and the institution knows that he or she has a high-rate credit card loan and also knows that that customer could qualify for a much lower interest rate home equity loan from an affiliated company.

If an opt-in restriction were in place, as in one of the California bills, you have a situation where someone would be punished for calling up and trying to tell the customer that he qualified for something that was of real benefit to him, because he did not opt-in at the beginning of this relationship.

Senator SHELBY. Mr. Kasper.

Mr. KASPER. Thank you, Senator Shelby.

That begs the question. We are here talking about banking products. What about insurance and securities products. An inducement to purchase an insurance product is called a rebate and it is illegal under almost all State insurance laws.

What about the small independent business people across the United States who are in the insurance and securities business as independent entrepreneurs trying to make a living competing with this inside information that is being passed around by the banks to their insurance organization to their securities organization?

It wipes out competition. It wipes out small business.

Our Nation is built on competition. This is anticompetition and the basis, the lifeblood of it is the free-flowing of this confidential information inside the financial conglomerates.

Where we are heading with this is thousands and thousands of businesses being out of business because we cannot compete.

Senator SHELBY. And fewer choices for the consumer.

Mr. KASPER. Absolutely fewer choices, Senator. Absolutely. The ones that benefit are the big institutions, not the consumer.

Senator SHELBY. Attorney General Hatch.

Mr. HATCH. Mr. Chairman, Senator Shelby, I believe the question was about the industry, are they reflecting the needs of their customers?

Exhibit A, what I filed, is a customer sheet. This is from Fleet Mortgage. These are their customer service reps and what they told the officers of Fleet Mortgage.

I just briefly have a couple of comments.

"Ninety-five percent of my calls pertain to people wanting to cancel their policies. I think we should have to get a signature."

Another one says, "They feel it is a fraud, it is a scam, they never wanted the insurance."

Another one is, "I think it is more hassle than it is worth."

Another one is, "I apologize for the inconvenience."

Another one is, "Customers should have to sign up for the products. Don't just add them to accounts."

And by the way, this is the company. This is an affiliate of the company.

The best one from an employee of Fleet Mortgage to its officers.

Chairman SARBANES. So these are some internal comments of the company.

Mr. HATCH. Oh, yes, internal.

Chairman SARBANES. Internal.

Mr. HATCH. I am hopefully not breaking too many laws here.

[Laughter.]

Chairman SARBANES. No, no, no. But I mean this is what they are saying to one another. It is like these stock analysts who tell people to buy the stock. And meanwhile, they are sending e-mails to one another saying what a turkey the company is.

Mr. HATCH. Correct. The best one is—this is from an analyst to the supervisor—I hope that Fleet Mortgage makes enough revenue from optional insurance to justify all the calls on our 800 line from customers trying to cancel.

Now is that an industry that is really representing its customers? I do not think so. In fact, I cannot find one comment—and this is their whole list—there is not one of them that is positive about what they are doing. They are all complaining.

Senator SHELBY. Mr. Chairman, I hope that as we go along with hearings, that we will get deeper into this and I hope that we can get some inside information like that.

I also want to mention, Mr. Chairman, that I saw—and I haven't talked with him—where Congressman John Dingell had initiated a probe into the tying of loans. In other words, I will loan you the money if you buy insurance or if you do so and so. I think that is something—because that is illegal. And that is something that I hope under your Chairmanship, that we will look into, also, because that does destroy competition in a big way.

Ms. Schlafly, do you have any comments on this?

Ms. SCHLAFLY. I do think that we should consider this a property rights issue.

Senator SHELBY. Absolutely.

Ms. SCHLAFLY. I mean, I believe I own the information about how I am spending my money and what I am planning to do.

Senator SHELBY. In other words, who does the information belong to?

Ms. SCHLAFLY. Right.

Senator SHELBY. Do you give it away? Is it gone? Gosh, if it does, the American people are going to be in for a shock, aren't they, a big, big shock.

One last question, Mr. Chairman. You have been very indulgent. How many signatures does it take to get a proposition on the ballot in California?

Mr. MIERZWINSKI. Senator, I actually do not know the exact number, but I can tell you that our organization has been involved in a number of them. It is a significant number, 1 percent or some-

thing of the people who voted in the last gubernatorial election across all of the counties.

We have been involved in a number of these and we are part of a group that is, along with I believe the California Office of Consumers Union, Consumer Action, a California-based group, Privacy Rights Clearinghouse, we are seriously considering going directly to the ballot. And by the way, the industry is split on this. There is one Internet bank that is a pro-privacy bank that is supporting the initiative, e-Loan Bank.

So, we are looking forward to working with an industry that actually believes that privacy is something that they can market.

Senator SHELBY. Mr. Kasper.

Mr. KASPER. Thank you, Senator Shelby.

When I was in California, I had the pleasure to meet Mr. Chris Larson, who is the Chairman of e-Loan.com, the bank that Ed Mierzwinski referred to.

The amount of signatures that they will need in California is between 700,000 and 900,000. He is so serious about this issue, that he has personally put up a million dollars of his own money to help get those signatures on the ballot. I understand the way the California initiatives work, you can actually hire people to get your signatures. So it is between 700,000 and 900,000.

Senator SHELBY. Mr. Chairman, thank you for your indulgence.

Chairman SARBANES. Thank you, Senator Shelby.

Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman.

Mr. Chairman, we seem to be listening to a choir that is singing the same song about a huge problem out there in America.

Chairman SARBANES. Well, there is some dissonant notes in this choir, I add.

[Laughter.]

Dr. CATE. Thank you, Mr. Chairman.

[Laughter.]

Senator AKAKA. There is a huge problem out there in America having to do with the privacy notices. I just happened to have a few here that I have been looking at. I have been reading and re-reading the notices. The notices are very complex and difficult to understand. What kinds of changes can be made to privacy notices to make them easier to understand? Also, what do the privacy notices fail to include that consumers should know?

If we can get feedback on these questions, that may help us in our quest to craft language that can help.

Mr. DUGAN. I would be happy to respond, Senator.

We agree with you that the privacy notices are more complicated than they should be. And as I said in my testimony, I think a real fundamental part of the problem is that there is always a tension with privacy notices about trying to give enough information to consumers to make an informed judgment, but not giving too much information so that people are confused and end up not reading the notices.

I think the regulators tried very hard to come out with things that simplified the requirements of the statute. But in the end, it turned out that what they proposed, and some of the sample clauses that they proposed and some of the legal terminology that

they used was very, very complicated. Indeed, some of the language that the Attorney General from Vermont quoted earlier was taken right out of these sample clauses.

Regulators recognize this, as does the industry. But the industry is in a bit of a Catch-22 because when they see what the regulators have put out and what they put in these sample clauses, they have to hew pretty closely to it because, if they do not, they fear exposure to legal liability.

And so, there is a question and there is, to be honest, some conservatism the first time out to go and do the letter of what was being prescribed, and in some cases, that came out sounding very legalistic and confusing.

I think since then, there has been very much an effort to try to deviate somewhat and keep within the spirit of the law.

But more importantly, there have been projects that the regulators have encouraged and the industry is now engaging in to try to come up with something that is simple, one page, that has common language terms, that language experts look at, that makes things easy to understand, to make the opt-out easy to understand and easy to exercise, and that people could use to compare among institutions.

That is not an easy process. It is going to take some time to try to develop and there are several different efforts underway. But we believe that is an important direction to try to explore, and that is what we would see as the way to go about trying to improve the notices because we do believe that that is a legitimate issue.

Senator AKAKA. Mr. Kasper.

Mr. KASPER. Thank you, Senator. I just jotted something down for your consideration.

If the question and the notice said something like this: Federal law allows us to share and sell your personal financial information for marketing purposes and marketing products. If you do not tell us not to, question, yes or no? Do you want us to be able to share or to sell your information without your written permission in advance? Yes or no. That would be simple.

Senator AKAKA. Yes.

Mr. KASPER. Bold letters, easy to understand. The consumer understands.

Ms. SCHLAFLY. How about a box to check?

Mr. KASPER. That is right. Yes or no. Check the box. That is exactly what I meant. Check the box, yes or no.

Senator AKAKA. Mr. Hatch.

Mr. HATCH. Mr. Chairman, Senator Akaka, I think that you get a very simple notice. People aren't going to respond to an opt-out. People do not read these things. There is no inducement for it.

In this country, we are used to an offer and an acceptance being an agreement. You have to have an affirmative act on both sides.

What we have done here is deviated from hundreds of years of commerce by saying that we are going to go to an opt-out. If the law was simply changed to saying, you cannot trade the information without permission, other than to serve the actual transactions involved, I guarantee you the bank, the credit card company, everybody, it would be very simple. It would be very clear, and they would offer something. And the consumer would respond to that

offer. It might be frequent flier miles. It might be—if, indeed, about \$300 is made off the sale of information on myself and on everybody else here in a year, and if 20 percent of it, if they offered that, some consumers are going to respond.

Yes, I do want my magazine subscriptions to be disclosed. No, I do not want my checks to be disclosed to other people. But give me the choice. It is my property. It is a personal liberty right.

If you have an opt-in, people will respond. There will be disclosure of information. It is just simply that people will pay for it. We are going to find out that it is a free enterprise system. It is a capitalist system, it should be. Let's let it work. They will make real clear disclosures. It will be clear. And they will even offer something for it.

Mr. SORRELL. I agree with General Hatch, that if opt-in was the standard, the industry that is struggling now to come up with simpler and more comprehensible privacy notices would find a way quickly to say clearly what the right is and make the case that it should be granted, that it wouldn't be eight pages into the notice and it wouldn't be using this language that somebody mentioned, you have to be a lawyer to understand it. This lawyer does not understand it.

So if opt-in was the standard, the industry would find a way, using its expertise, to make the most compelling case, to convince the consumer why it is in the consumer's best interest to give this permission.

We have, as I think was said before, only minuscule privacy-related complaints post-Gramm-Leach-Bliley. The reason for that is because the average consumer doesn't understand the notices, doesn't understand what the industry is doing in terms of the sharing of information right now.

These battles are not over in the State capitals. It is literally just beginning. Efforts by this Committee and comparable committees in State capitals around the country, this thing is just starting.

Mr. MIERZWINSKI. Senator, I agree with the two Attorneys General that opt-in is the right way to go. Without opt-in, you need to improve the notices by going to something like an express statutory language that appears in a box, as General Sorrell suggested earlier, similar to the nutrition box on the front of the notice. Because the only right you have is the limited right to say no to some of the sharing. But most of the notices put that at the end of the eight pages. The right has to be moved forward and then needs to be marketed by the agencies. And the legal gobbledygook and double-speak needs to be eliminated.

Senator AKAKA. Yes, Dr. Cate.

Dr. CATE. Senator, two responses, if I may.

First, I think we have to distinguish the setting in which you are talking about consent being obtained.

If we are talking about the opt-in or opt-out or whatever the choice is being on the document that opens the account or you apply for the loan, clarity of the notice will I think undoubtedly come and getting consumers to respond is comparatively easy because they have to respond. They have to do something to move on.

What Gramm-Leach-Bliley did and what I think is of greater concern, is to apply a requirement to data that has already been

collected, so consumers who are not coming to an institution looking for service, but rather, requiring the institution to go out to the consumer. We know that it is very difficult and enormously intrusive to the consumer to actually reach them.

There are many studies, there is testimony before the Federal Communications Commission, there have been court cases on this about the number of phone calls it takes, the number of letters it takes, and the fact that adding money to the offer makes absolutely no difference statistically. For example, the Post Office tells us that unsolicited commercial mail, not first-class mail, but unsolicited commercial mail, that half, 52 percent of those are thrown away without being opened. So it won't matter how many \$5 bills you stuff in the envelope. If they are thrown away without being opened, it is going to be very difficult to get consent, no matter what the consent system is.

The first point is that it is critical to keep in mind here the difference between the settings in which we might ask for consent. The second point is the question of liability related to notice.

It would be much easier to write standardized notices, which I think were suggested earlier and are a terrific idea, notices you could compare across institutions like food labeling.

The problem right now is that all of the information you have to explain to comply with the law, and if you explain inaccurately in any degree, you are liable. It is a strict liability standard.

So if you say, "no, we do not share your information with third parties," but it turns out you actually have a processing service that does work for you under contract, even though it cannot do anything with the information other than process it, that violates the terms of the notice.

Then you get these complicated statements—"we do not share information with third parties, other than for processing purposes"—and these lengthy explanations.

If we move to a common sense regulatory system, if the FTC, for example, were empowered to develop a system of basic questions that consumers would find the answers useful to—"Do you share information with third parties for marketing? Yes or no?" That would be a question that I think all of us would understand the answer to, and I think frankly that is what many of us care about.

We are not actually interested in who processes your payroll or who processes your checks. We want to know, "Are you sharing the information so that I am going to be getting mail."

That type of notice offers tremendous opportunities because it also allows for real customization. You can say, not only "Do you want to hear from us or not," but also you can say, "Do you want to hear from us by e-mail? Do you want to hear from us by mail?"

We can actually allow a tremendous amount of consumer choice. But we are going to have to back away from this very complex strict liability regime to make that work.

Senator AKAKA. Mr. Kasper, did you have a comment?

Mr. KASPER. I did, Senator. Thank you.

I just wanted to be sure the record reflected, in responding to your question about what the notice should say. That does not mean that I agree that that is what the notice should be. I support no-opt for affiliate-sharing and opt-in for nonaffiliate-sharing.

The comments from the industry spokesmen begs to ask, are you assuming, then, that the people of the United States are sitting at home breathlessly waiting for their telephone to ring so that they can buy something from you on the telephone that they neither want, nor need?

I happen to believe that the answer is no. People will buy when they want, from whom they want, and what they want, if they are left alone. This bombardment by the telemarketing organizations and the banking organizations assumes that the people want the stuff. They do not want it. They do not want to be intruded upon. They want to be left alone.

Senator AKAKA. Mr. Chairman, I know that my time is up. I just want to mention that next year, we may be considering the Fair Credit Reporting Act. We will need to look at possible changes in the legislation to ensure that consumers have the necessary privacy protections.

Thank you very much, Mr. Chairman.

Chairman SARBANES. Thank you very much, Senator Akaka.
Senator Carper.

COMMENTS OF SENATOR THOMAS R. CARPER

Senator CARPER. Thank you, Mr. Chairman.

To our witnesses, welcome. We thank you for your testimony today and for your response to the questions that are being posed.

When Congress was debating and finally passing Gramm-Leach-Bliley, I was back in Delaware trying to govern the State as their Chief Executive and I did not participate in the debate here or in the conference.

I do not know if any of you are comfortable in taking us back a couple of years to the time when that debate was ongoing and the compromise was worked out, which is now part of the law of the land. And just take a minute and tell this old governor, how did we end up with the compromise that we now have?

Mr. DUGAN. Well, I was involved at the time representing financial institutions.

I think—and this is just one person's view of how this came about—that there was, in fact, tremendous concern about imposing an opt-in regime and that, on the other hand, I think there was true concern about when information is shared outside a corporate family, and it led to the notion that something should be done to provide consumers with control when information gets shared outside of a corporate family.

That is where the debate first started about providing—some people wanted to go further and some people thought that we did not need anything. But that is where Congress struck the balance and said, we should allow consumers the right, make institutions give consumers the right, to opt-out for sharing outside of the corporate family.

On the other hand, smaller financial institutions came in and said, that is not quite fair because for us to compete and offer a range of financial services, there are relationships that we have to enter into, joint marketing relationships with other financial institutions—not just any company, but other financial institutions—in order to survive, and we have to be put on the same footing, the

same playing field as affiliates. That is what caused the creation of the joint marketing exception for the sharing of information with other financial institutions.

Congress also imposed strict limits on the redisclosure and reuse of information, however it was shared. There was also tremendous debate—when this thing got started, everybody thought it was simple, but there were many, many kinds of information that needed to be shared, and not just to carry out a transaction. The law recognized a whole host of exceptions from the opt-out restriction, these exceptions were very suspiciously viewed at the time, but turned out to be very wisely put in and have not been controversial since then. For example, sharing information with regulators, for judicial process, to detect fraud, to share with credit bureaus, etc.

That was the basic structure that was put in place. The notion also was, you had to have notices because opt-out only works if you have meaningful notices, and you had to have a regulatory scheme to enforce it and actually write detailed regulations about it.

What has happened since then is that this is the first time that the Government has written such detailed privacy regulations. In a sense, the financial services industry has been something of a guinea pig in that you have very detailed regulations being written for the first time where people had to struggle on how these kinds of things were sorted out and a number of decisions were made.

I think a lot of progress was made, but, obviously, as I mentioned in context with the notices, there are more improvements that could be made.

Senator CARPER. General Hatch.

Mr. HATCH. Mr. Chairman, Senator Carper, this is my recollection and it is from the hinterland. So, I could be totally wrong and I am sure the Chairman has a much better recollection of how this privacy provision got into play. But in the hinterland, in June, I sued a bank, U.S. Bank, and alleged that they had taken a million depositors and sold 22 pieces of information to telemarketers, making a lot of money on this thing.

The day before, the OCC Chairman Hawke had given a speech in San Francisco, and he had been harping about this for years, saying, banks, you have to clean up your act.

They are all denying it.

So the day afterwards—they all denied it—we filed the suit. Very clearly, we were in communication with the OCC on this issue. We filed the suit, and I will never forget it. On Wednesday, all the banks said, oh, we are not doing this. Just U.S. Bank.

By Thursday, all of them were saying, I guess we are doing it. We are not going to do it any more, because we were basically saying, it was consumer fraud because they had said that there was a right to privacy in their literature. We were also alleging a common law right to privacy with regard to financial data.

They were disclosing, for instance, your high balance, your low balance, all sorts of information from whence, you know, a telemarketer will know when to hit you, which day of the month, how much disposable income you have, what your age is. And, as I mentioned earlier, two-thirds of this is targeted to the senior citizens.

We were plowing through on this suit, and the bank came in and we started doing some negotiation. We had an opt-in agreed.

But then, I get a call and I am told that the GLB, Gramm-Leach-Bliley, is going through, which had nothing to do, to my knowledge, with privacy. The Chairman would know better than I. But my understanding was that it did not have anything to do with privacy at that time.

There was a grand debate over Glass-Steagall that was passed in 1933, and the Douglas Amendment that was passed in 1956 with regard to what banks, what business they could get into.

And next thing I know, all these banks are plowing into Minnesota, or at least these lobbyists plowing in, all these threats and no, you cannot settle this thing with an opt-in. Congress is going to preempt everything.

But for the Chairman's amendment, everything we were involved with then would be worthless.

I do not think this was any great thought-out privacy act. But for the efforts to hold it off and allow the States to do something, it was just simply a way to get around killing the right to privacy as it relates to banks. Maybe I am wrong.

Chairman SARBANES. Well, for the sake of full and of fair disclosure—

[Laughter.]

—we should register that the position of the industry at the time was that there should be no privacy protection. That was their basic position.

Now, what we ended up with in the bill was, there was an effort made to try to deal with the privacy issue and we got what I regard as some minimal provisions. But also, in light of the fact that they were so minimal, we were able to get a provision in, an explicit provision, that the States could go beyond the Federal.

My own view is that if we had not gotten that provision in, that we would still not have preempted. But it would have left open the argument to be made, which I am sure the industry would have made, that simply putting the standard, the minimal standards, in constituted a preemption, even though the legislation might not have said that there was a preemption.

In any event, we were able to avoid all of that by getting the explicit provision that the States can go beyond, and therefore, I think, saving the Attorneys General a lot of litigation that otherwise would have occurred, asserting that the minimal standards in Gramm-Leach-Bliley constituted a preemption.

But to put all of this into perspective, the industry's position at the time that we were considering this legislation was that there should be no privacy protections.

Mr. Dugan, I have to say to you and your clients here today that this issue has not reached a point of equilibrium or a point of repose, in my judgment. In other words, I do not think that the current provisions about privacy protection are perceived by most people as being adequate.

Therefore, I think this issue is going to remain on the agenda. And it seems to me that it behooves those that are interested in it to start thinking in a positive and constructive way about what the system could be that would provide the extent of protection that most people would conclude is appropriate, that puts the issue to rest and might well encompass within it accommodations for

some of the administrative things that the industry is concerned about. At least that should be examined and considered.

Otherwise, it is my prediction that if we continue along in the current path, there will be the equivalent of Enron and Worldcom one of these days in the privacy field, and you may well end up with a regime which you say, oh, how did we ever get to this point? And the answer is going to be, you got there because you weren't trying to work through to a positive and rational solution.

Now, I want to commend the Attorneys General for the interest they have taken. It is extremely important. And I know the two of you are only reflective of many others in other States across the country who have interested themselves in this issue.

Mr. Kasper, certainly you contributed immeasurably by coming here today and telling us the North Dakota experience. Of course, Mr. Mierzwinski has been working on this issue.

Ms. Schlafly, I have to say, you added this property dimension issue, property rights dimension. It is a very interesting dimension. I had not really thought about it as much as I probably should have until you started speaking here today. It is very interesting.

If it means so much economically to these institutions to get this information and use it, obviously it has some kind of property value. It starts out coming from the consumer. That value should be protected or at least compensated for, perhaps. It raises a very interesting question, over and above the basic privacy issues.

Anything else, Senator Carper?

Senator CARPER. Just one last thing, if I could. I am going to ask if maybe Mr. Dugan would just reply for the record and not here today because the hour is late.

My wife is from North Carolina. A member of her family's identity was stolen, a victim of identity theft. Probably everybody here knows someone personally who has gone through what she has gone through. It has not been fun.

And just in the last week, I get a weekly report from a person on my staff in Delaware who heads up constituent services for me. We are beginning to see a growing number of people who call our office because they too are victims of identity theft.

The question I am going to ask, perhaps, for Mr. Dugan—I do not mean to pick on you, but just for the record, if you could let me know what steps you are aware of that the financial services industry is taking to help combat this problem.

Mr. DUGAN. I would be happy to do that, Senator. And I do just want to say, very briefly, that you raise a very good point.

That is precisely the kind of thing, we do think that that is a real issue. And it is that kind of issue that, if there is a need, should be addressed, that there is legislation that needs to be done to take some steps in that direction. That is something, a targeted kind of harm where there is a problem. Then we should try to come up with things that go right at that, as opposed to something very nebulous and broad-based about information-sharing generally, to try to get at the same thing.

But we would be happy to respond.

Senator CARPER. Thank you.

Mr. MIERZWINSKI. Senator, if I could add briefly. From the consumer groups' perspective, identity theft results largely from a fail-

ure of the big banks, the credit card companies, and the credit bureaus to adhere to all of the Fair Information Practices and take care of our information.

It is too easy for a thief to represent themselves as me. All they need is my Social Security number, a very poor unique identifier, and my name. And then they apply in my name. The credit bureau gives the bank a copy of a credit report that says, he passes, and then the credit card is mailed to the wrong guy.

That is how easy it is.

We consider this debate over opt-in and opt-out sometimes covers up all of the other issues related to privacy. But how the institutions take care of information is just as important.

Senator CARPER. Thanks, Mr. Chairman.

Chairman SARBANES. I may note as we draw to a close that the European Union has developed privacy protections well beyond anything that we have here.

American companies are trying to meet an adequacy standard. They have not been able to do that yet. They may have to go to Safe Harbor, which they do not want to do because they would have to elevate the protections they provide. But I am increasingly concerned about this. The EU is a growing economic force, and its size, both in terms of population and gross national product compares with the United States.

If we are not careful, many of the advantages that we have had as the economic leader, and I think, suppose the EU moves ahead with better privacy protections. They seem to be moving ahead with better accounting standards, although we may now be able to remedy that situation.

But they have this accountability—we used to say to them, you have to do American-style accounting because that is the best in the world, the most transparent. We have the best integrity of the markets. And now they are saying to us, what?

[Laughter.]

They are out there trying to compete with us because we are falling short. These issues have far-ranging implications, I think. And this does not strike me as the issue that you are either here or you are there.

There is obviously a whole area in which we can work to try to reach a reasonable solution. But I do think if we are going to do that, we have to move significantly back in the direction that our starting point is that this information belongs to the individual who provides the information. And then you go from there in terms of what uses can be made of it and the individual's involvement in making that judgment.

We want to thank all of you for coming. This has been an extremely helpful panel. We appreciate the time and the effort that each of our witnesses gave in preparing for it.

The hearing stands adjourned.

[Whereupon, at 12:35 p.m., the hearing was adjourned.]

[Prepared statements and additional material supplied for the record follow:]

PREPARED STATEMENT OF WILLIAM H. SORRELL

ATTORNEY GENERAL, STATE OF VERMONT

SEPTEMBER 19, 2002

Good morning, and thank you for inviting me to speak with you today on the important issue of financial privacy. I would like at the outset to recognize and express my gratitude for the critical role played by this Committee in the protection of consumers' financial privacy. Unfortunately, the Gramm-Leach-Bliley Act (GLB)¹ does not protect consumers' financial privacy as intended by this Committee. I recommend that this Committee take further action to ensure that its previous good work results in real protections for consumers.

In these comments I address the following topics:

1. The inability of GLB, as currently construed by Federal regulators, to stop the abusive telemarketing practices that gave rise to the financial privacy provisions of GLB in the first instance.
2. The inability of consumers to exercise their rights under GLB because industry notices are incomprehensible.
3. The problems associated with sharing of financial information among corporate affiliates.
4. The need to allow States to continue to address problems associated with sharing of financial information both among affiliates and nonaffiliated third parties.
5. Recommendations for Congressional action in these areas.

GLB Does Not Protect Consumers From Harms Associated With Sharing Nonpublic Financial Information

Congress intended Title V of GLB to protect consumers from abuses associated with sharing of nonpublic personal financial information. As a result of enforcement actions brought by State Attorneys General against information-sharing practices of major banking institutions, Congress created Title V to protect consumers with respect to such sharing of their financial information. However, the provisions of Title V are insufficient to protect consumers from the harms associated with these practices, and pose considerable risks to consumers. The provisions that allow financial institutions to share encrypted account numbers and other forms of billing information for marketing purposes are particularly troublesome. Moreover, the notices issued by financial institutions under GLB have been dense and require a high reading level to comprehend, resulting in consumer confusion and inability to exercise informed choice. Congress should act to correct these problems, thus ensuring Title V's capacity to protect consumers in the area of financial privacy.

GLB Does Not Protect Consumers From Fraudulent Telemarketing

The information held by financial institutions about their customers is highly valuable. While financial institutions might not disclose this highly valuable information to their competitors, they do disclose this information to marketing partners and to third parties for the purpose of jointly marketing products and services unrelated to the customers' current service selection, and even unrelated to the particular type of services performed by the financial institution itself. The harm to a consumer resulting from this type of information-sharing stems from the tactics sometimes used in marketing new products to the consumer, who usually does not realize that the marketer already has the consumer's credit card number, or access to the credit card account through an encrypted number or other unique means of identification.

Indeed, it was well known in 1999 that practices of sharing customer financial information by major banking institutions facilitated these telemarketing abuses. In the spring of 1999, the Minnesota Attorney General announced a settlement with U.S. Bancorp, resolving allegations that U.S. Bancorp misrepresented its practice of selling highly personal and confidential financial information regarding its customers to telemarketers. One year later, thirty-nine additional States and the District of Columbia entered into a similar settlement.² The States' investigation focused on the bank's sale of customer information—including names, addresses, telephone numbers, account numbers, and other sensitive financial data—to marketers. Based on this confidential information, the marketers made telemarketing calls and

¹Pub. L. No. 106-102 (1999).

²The basis for the States' action was their charge that U.S. Bancorp misrepresented its privacy policy to its customers. In some account agreements provided to its customers, the bank listed the circumstances under which information would be disclosed, but failed to include any reference to the bank's practice of providing such information to vendors for direct marketing purposes.

sent mail solicitations to the bank's customers in an effort to get them to buy the marketers' products and services, including dental and health coverage, travel benefits, credit card protection, and a variety of discount membership programs. Buyers were billed for these products and services by charges placed on their U.S. Bancorp credit card. In return for providing confidential information about its customers, U.S. Bancorp received a commission of 22 percent of net revenue on sales with a guaranteed minimum payment of \$3.75 million.

As a result of the evidence uncovered through the U.S. Bancorp case, Congress intended to limit the ability of financial services companies to sell or give their customers' nonpublic personal information to third-party telemarketers. Congress intended to forestall these abusive telemarketing practices by specifically prohibiting financial institutions from sharing an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer with any nonaffiliated third-party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.³

However, the regulations adopted to implement GLB allow financial institutions to sell or to share *encrypted* credit card numbers or other unique identifiers, which enables the telemarketing abuses that were at the heart of Congressional concern to continue unabated. The Federal agencies' rules implementing this section on sharing of account numbers sets forth two "examples," the first one of which states:

ACCOUNT NUMBER. An account number, or similar form of access number or access code, *does not include a number or code in an encrypted form, as long as the bank does not provide the recipient with a means to decode the number or code.* CFR §40.12(c) [emphasis added].

Thus, a telemarketer or other recipient of an encrypted account number or unique identifier is able to notify a financial institution that a particular consumer indicated a desire to purchase an item, thus causing the consumer's account to be charged, without ever asking the consumer for permission to charge the account. The financial institution then uses its decode mechanism, which it never shares with an unaffiliated party, to determine which account to charge. This type of marketing is known as "preacquired account" telemarketing. The possibility of unauthorized charges and fraudulent practices in such circumstances is greatly increased over situations where the consumer must affirmatively give a credit card number for the account to be charged.

Preacquired account telemarketing is inherently unfair and susceptible to causing deception and abuse, especially with elderly and vulnerable consumers. Preacquired account telemarketing turns on its head the normal procedures for obtaining consumer consent. Other than a cash purchase, providing a signature or an account number is a readily recognizable means for a consumer to signal assent to a deal. Preacquired account telemarketing removes these shorthand methods of consumer control. The telemarketer not only establishes the method by which the consumer will provide consent, but also decides whether the consumer actually consented.

The Federal Trade Commission, in its recent Notice of Proposed Rulemaking regarding the Telemarketing Sales Rule, has proposed prohibiting "preacquired account" telemarketing.⁴ Forty-nine States, the District of Columbia, and three Territories recently filed comments with the Federal Trade Commission that strongly support this proposal.⁵ In their comments, these States, Territories, and the District of Columbia noted that the consequence of this fundamentally unfair selling method is clear: Consumers are assessed charges for products they did not want, and did not understand they were purchasing.

Fleet Mortgage Corporation, for instance, entered into contracts in which it agreed to charge its customer-homeowners for membership programs and insurance policies sold using preacquired account information. If the telemarketer told Fleet that the homeowner had consented to the deal, Fleet added the payment to the homeowner's mortgage account. Angry homeowners who discovered the hidden charges on their mortgage account called Fleet in large numbers.⁶ . . . Approximately one-fifth of all calls by Fleet customers were about these preacquired account "sales." Customers over-

³ Gramm-Leach-Bliley Act, Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1338, Section 502(d).

⁴ 67 Fed. Reg. 4491.

⁵ Comments of 52 Attorneys General, the District of Columbia Corporation Counsel, and the Hawaii Office of Consumer Protection Regarding Proposed Amendments to the Telemarketing Sales Rule, April 12, 2002, available at www.naag.org.

⁶ The mortgage statements issued by Fleet hid the charges under the rubric "opt.prod." at the very bottom of the bill in small print, such that it was extremely difficult to discover the charge or discern the purpose of the charge. For consumers on auto-draft from their checking or other bank account, Fleet gave no written notice of the charge.

whelmingly told Fleet that they did not sign up for the product, and wanted to know how it was added to their mortgage accounts without their approval, consent, or signature.⁷

This Committee should take the lead in protecting consumers from such abusive telemarketing practices by prohibiting the use of encrypted numbers, unique identifiers, and other means for accessing a consumer's account.

Moreover, it seems likely that, as information-sharing increases, the risk of misuse or misappropriation of such information increases as well. It may well be that the greater the quantity and level of detail of confidential information, and the more entities that possess such information, the higher the chance that the information will be stolen or misappropriated, or used for other inappropriate purposes, such as the improper denial of credit, insurance, or employment. I therefore urge this Committee to look beyond the known risks of telemarketing abuses to identify and evaluate less obvious risks, including potential identity theft.

GLB Notices are Inadequate to Advise Consumers of Their Rights With Respect to Information Sharing

The notices to consumers that are required under GLB⁸ are woefully inadequate. Consumers have been greatly confused by the dense information in the notices, which require a high education level to comprehend. As a result, consumers have not been adequately informed about their rights to opt-out of information-sharing with third parties.

The opt-out notices provided by financial institutions in their effort to comply with GLB have not been "clear and conspicuous," as those terms are commonly understood. Opt-out notices mailed by many financial institutions have been unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans.⁹ Experts have highlighted the inadequacy of such statements. Mark Hochhauser, Ph.D., a readability expert, reviewed sixty GLB opt-out notices. Dr. Hochhauser determined that these notices were written at an average third or fourth year college reading level, rather than the junior high level comprehensible to the general public.¹⁰ For example, the notice sent to customers by one financial institution stated:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt-out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law).¹¹

Recent surveys demonstrate that consumers either never see and read such complicated opt-out notices, or they do not understand them. A survey conducted by the American Bankers Association¹² found that 41 percent of consumers did not recall receiving their opt-out notices, 22 percent recalled receiving them but did not read them, and only 36 percent reported reading the notice. Another survey, conducted by Harris Interactive for the Privacy Leadership Initiative, announced its results in early December 2001.¹³ The Harris Survey indicated that only 12 percent of consumers carefully read GLB privacy notices most of the time, whereas 58 percent did not read the notices at all or only glanced at them. The Harris Survey further indicated that lack of time or interest *and* difficulty in understanding or reading the notices top the list of the reasons why consumers do not spend more time reading them.

Those consumers that do read the GLB notices have voiced numerous complaints, raising concerns that the financial institutions' unintelligible notices are an attempt to mislead them.¹⁴ The opt-out approach promulgated under GLB has proven so problematic that the Federal agencies that administer the regulations under GLB convened an Interagency Public Workshop to address the concerns that have been raised "about clarity and effectiveness of some of the privacy notices" sent out under

⁷ Comments of 52 Attorneys General, the District of Columbia Corporation Counsel, and the Hawaii Office of Consumer Protection Regarding Proposed Amendments to the Telemarketing Sales Rule, *supra* note 5.

⁸ 15 U.S.C. § 6802(b)(1)(A).

⁹ See Robert O'Harrow, Jr., "Getting a Handle on Privacy's Fine Print: Financial Firms' Policy Notices Aren't Always 'Clear and Conspicuous,' as Law Requires," *The Washington Post*, June 17, 2001, at H-01.

¹⁰ Mark Hochhauser, Ph.D., "Lost in the Fine Print: Readability of Financial Privacy Notices," <http://www.privacyrights.org/ar/GLB-Reading.htm> (2001).

¹¹ See Hochhauser, *supra* n. 10.

¹² Available at <http://www.aba.com/Press+Room/bankfee060701.htm>.

¹³ Available at <http://www.ftc.gov/bcp/workshops/glb> (hereinafter "Harris Survey").

¹⁴ Harris Survey, *supra* n. 13.

GLB.¹⁵ The agencies noted that consumers have complained that “the notices are confusing and/or misleading and that the opt-out disclosures are hard to find.”¹⁶

Where the vast majority of consumers do not even read opt-out notices, and those who read the notices cannot understand them, it cannot be said that they are able to understand their rights and exercise their choices intelligently. As a result, the Attorneys General of forty-two States, the District of Columbia, and two Territories called on the FTC and other Federal regulatory agencies to create standard notices and require much simpler language so that consumers can understand them.¹⁷

Congress should step in and require the Federal agencies to create standard notice forms for use by the financial services industry under GLB. Standard notices for financial privacy could be modeled on the nutritional labeling required by the Congress under the Nutritional Labeling and Education Act. Use of such standard notices would enable consumers to much more easily understand their rights, and to exercise their choices allowed under Federal law.

The FCRA Does Not Adequately Protect Consumers From Abuses Associated With Sharing of Nonpublic Personal Financial Information Among Affiliates

The concerns with respect to sharing of information with unaffiliated third parties—abusive telemarketing practices and incomprehensible notices—apply with equal force with respect to sharing of nonpublic personal financial information among corporate affiliates. The breadth and number of affiliates of some financial institutions is breathtaking, yet most consumers remain unaware of the existence or identity of their financial institutions’ affiliates. Consumers should be better protected from the harms associated with affiliate-sharing by giving consumers an effective choice before credit-related information can be shared throughout a vast corporate complex.

Under the FCRA, consumers have no choice as to whether their transaction and experience information will be shared with their financial institution’s corporate affiliates. Moreover, once they are given a notice and opportunity to opt-out, all other information can also be shared with the corporate affiliate group. Thus information about the consumer’s income, employment history, credit score, marital status, and medical history can be shared with ease among corporate affiliates.

GLB greatly expanded the activities that were permissible under one corporate umbrella, as it allowed insurance, securities, and banking institutions to affiliate with each other. Even prior to enactment of GLB, financial institutions were allowed to affiliate with a broad spectrum of companies. The list of activities that are identified by the Federal Reserve Board in its rulemaking as “financial” in nature or closely related to financial activities, and therefore permissible for inclusion within a financial holding company, goes well beyond traditional financial activities, and includes the following:

- Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State.
- Providing financial, investment, or economic advisory services, including advising an investment company (as defined in Section 3 of the Investment Company Act of 1940).
- Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.
- Underwriting, dealing in, or making a market in securities.
- Leasing real or personal property (or acting as agent, broker, or advisor in such leasing) without operating, maintaining, or repairing the property.
- Appraising real or personal property.
- Check guaranty, collection agency, credit bureau, real estate settlement services.
- Providing financial or investment advisory activities including tax planning, tax preparation, and instruction on individual financial management.
- Management consulting and counseling activities (including providing financial career counseling).
- Courier services for banking instruments.

¹⁵ Interagency Public Workshop, “Get Noticed: Effective Financial Privacy Notices,” <http://www.ftc.gov/bcp/workshops/glb/>; see also Press Release, “Workshop Planned to Discuss Strategies for Providing Effective Financial Privacy Notices,” <http://www.ftc.gov/opa/2001/09/glbworkshop.htm> (September 24, 2001).

¹⁶ See Joint Notice Announcing Public Workshop and Requesting Public Comment, “Public Workshop on Financial Privacy Notices,” at 3.

¹⁷ See Comments of 44 Attorneys General to Federal Trade Commission Regarding GLB Notices, dated February 15, 2002, available at www.naag.org.

- Printing and selling checks and related documents.
- Community development or advisory activities.
- Providing financial data processing and transmission services, facilities (including hardware, software, documentation, or operating personnel), databases, advice, or access to these by technological means.
- Leasing real or personal property (or acting as agent, broker, or advisor in such leasing) where the lease is functionally equivalent to an extension of credit.
- Providing investment, financial, or economic advisory services.
- Operating a travel agency in connection with financial services.¹⁸

Thus the types of businesses with which traditional financial institutions may now affiliate themselves, in addition to banking, insurance, and securities brokerage, include:

- mortgage lenders;
- “pay day” lenders;
- finance companies;
- mortgage brokers;
- account servicers;
- check cashiers;
- wire transferors;
- travel agencies operated in connection with financial services;
- collection agencies;
- credit counselors and other financial advisors;
- tax preparation firms;
- non-Federally insured credit unions; and
- investment advisors that are not required to register with the Securities and Exchange Commission.¹⁹

Also included among the list of permissible affiliates are institutions that are “significantly engaged in financial activities,” such as:

- A retailer that extends credit by issuing its own credit card directly to consumers.
- A personal property or real estate appraiser.
- An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days.
- A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization or individuals who are currently employed by or seeking placement with the finance, accounting or audit department of any company.
- A business that prints or sells checks for consumers, either as its sole business or as one of its product lines.
- An accountant or other tax preparation service that is in the business of completing income tax returns.
- An entity that provides real estate settlement services.²⁰

The number and breadth of affiliates currently associated with some of the country’s major financial institutions is astounding. Submitted with these comments for the Committee’s official record are the corporate affiliate lists for Bank of America Corporation, Citigroup, Inc., and KeyCorp,²¹ which serve as three examples of the level of affiliation at large- and mid-sized banking institutions in this country. Bank of America lists 1,476 corporate affiliates; Citigroup lists 2,761 corporate affiliates; and KeyCorp lists 871. A perusal of these corporate affiliate lists demonstrates that these holding companies appear to be involved in widely disparate activities, including insurance, securities, international banking, real estate holdings, and development, and equipment leasing. Some of these affiliate operations may, in the normal course of their business, gather highly personal health information about consumers. A consumer holding a credit card with the lead bank or a property and casualty insurance policy with a major insurer in any of these affiliate groups would

¹⁸ Examples 1–4 are from 12 U.S.C. § 4(k); examples 5–13 are from 12 CFR § 225.28; and examples 14–16 are from 12 CFR § 211.5(d).

¹⁹ 16 CFR § 313.1 (b).

²⁰ 16 CFR § 313.3 (k)(2).

²¹ These lists, and other corporate affiliate lists for bank holding companies can be obtained at [http://132.200.33.161/nicSearch/servlet/NICServlet?\\$GRP\\$=INSTHIST&REQ=MERGEDIN&MODE=SEARCH](http://132.200.33.161/nicSearch/servlet/NICServlet?GRP=INSTHIST&REQ=MERGEDIN&MODE=SEARCH).

not expect that his or her transaction and experience information would be spread throughout the corporate affiliate structure for the purpose not of servicing the consumer better, but of marketing products to the consumer.

The only appropriate mechanism for giving consumers control over sharing of information within such broad affiliate groups is to require that consumers be given effective notice and choice before their information may be shared with affiliates.

Unfortunately, current notices to consumers about their rights under the FCRA with respect to sharing of nonpublic personal financial information with affiliates are highly inadequate, just like the notices about consumers' rights under GLB. Indeed, both GLB and the FCRA require that notices about information-sharing practices and information about how consumers can exercise their opt-out rights must be written in a "clear and conspicuous" manner.²² The Federal regulatory agencies have not yet issued any guidance on how these two notice requirements work together. Many financial institutions have incorporated their affiliate-sharing notices required under the FCRA within their notices about the sharing of information with unaffiliated third parties required under GLB. Consumers have experienced the same problems outlined previously, with respect to affiliate-sharing notices as they have experienced with notices about sharing of information with unaffiliated third parties.

Accordingly, Congress should require financial institutions to give consumers an effective choice before nonpublic personal financial information can be shared among affiliates. Moreover, Congress should direct that the standard financial privacy notices to be created by the Federal regulatory agencies contain a standard format for information about affiliate-sharing practices and consumers' choices to control such sharing.

Congress Should Continue to Allow States to Enact More Protective Laws With Respect to Financial Privacy

Prior to GLB, States had enacted provisions relating to financial privacy that were more protective than the provisions of Federal law. This Committee ensured the ability of States to continue to protect their citizenry by enacting Section 507 of GLB, which allows States to adopt financial privacy laws relating to sharing with unaffiliated third parties that are more protective than Title V. Due to the inadequacies of GLB discussed above, States and localities have been exercising this authority to ensure that their consumers' financial information is protected. Moreover, under the FCRA, the current preemption of more protective State laws relating to affiliate-sharing is due to sunset on December 31, 2003.

This Committee should ensure that States continue to be entitled to enact more protective laws with respect to sharing of financial information with third parties and affiliates.

State Law on Information Sharing With Unaffiliated Third Parties

Recognizing that many of the problems inherent with GLB stem from the Federal law's acceptance of consumer "opt-out" as an appropriate means of registering consumer choice, States and local governments have been actively adopting laws that require consumers to opt-in before their information can be shared. There are currently six States that have enacted laws that require some form of opt-in before financial information can be shared by banks.²³ Fourteen States have enacted laws or regulations that require some form of consumer consent before financial information can be shared by insurance companies.²⁴ In addition, North Dakota voters recently adopted a referendum reversing the State legislature's repeal of that State's opt-in law, putting that State's banking opt-in law back on the books. Two California localities—San Mateo County and Daly City—also have recently adopted ordinances requiring affirmative consumer consent before financial information can be shared. These laws are a reaction by State and local governments to the problems

²² 15 U.S.C. § 6802(b)(1)(A); 15 U.S.C. § 1681a(d)(2)(A)(iii).

²³ Alaska (ALASKA STAT. § 06.05.175); Connecticut (CONN. GEN. STAT. ANN. § 36a-42); Illinois (205 ILL. COMP. STAT. ANN. 5/48.1); Maryland (MD. CODE ANN., Financial Institutions § 1-302); North Dakota (N.D. CENT. CODE § 6-08.1-04); and Vermont (VT. STAT. ANN. tit. 8, § 10201 and BISHCA Regulation B-2001-01).

²⁴ Arizona (ARIZ. REV. STAT. ANN. § 20-2113); California (CAL. INS. CODE § 791.13); Connecticut (CONN. GEN. STAT. ANN. § 38a-988); Georgia (GA. CODE ANN. § 33-39-14); Maine (ME. REV. STAT. ANN. tit. 24-A, § 2215); Massachusetts (MASS. GEN. LAWS ANN. ch. 175I, § 13); Minnesota (MINN. STAT. ANN. § 72A.502); Montana (MONT. CODE ANN. § 33-19-306); Nevada (NEV. ADMIN. CODE ch. 679B §§ 679B.560-679B.750); New Jersey (N.J. STAT. ANN. § 17:23A-13); New Mexico (N.M. ADMIN. CODE tit. 13, §§ 13.1.3.1-13.1.1.28); North Carolina (N.C. GEN. STAT. § 58-39-75); Ohio (OHIO REV. CODE ANN. § 3904.13); Oregon (OR. REV. STAT. § 746.665); and Vermont (VT. BISHCA Regulation IH-2001-01).

associated with GLB, and an effort by these governments to provide consumers with protections greater than those afforded under Federal law.

Some States have adopted laws or regulations that are designed to address some of the specific problems consumers face under Federal law. For example, Vermont's new financial privacy regulations specifically prohibit banks, insurance companies, and securities firms from sharing encrypted account numbers or other unique identifiers that would allow telemarketers and others to access a consumer's account. See, that is, Vermont Department of Banking, Insurance, Securities, and Health Care Administration Regulation B-2001-01, Section 13 (available at <http://www.state.vt.us/atg/Banking%20Adopted%20Rule.pdf>).

Congress should ensure that States can continue to be allowed to protect their consumers with respect to sharing of financial information with third parties by enacting laws that are more protective than GLB's Title V.

State Law on Affiliate Sharing

Similarly, Congress should ensure that States can adopt laws that are more protective than the FCRA with respect to affiliate-sharing. The FCRA prohibits States from enacting or enforcing provisions with respect to sharing of information among affiliates until January 1, 2004.²⁵ Congress should allow this preemption provision to sunset, as scheduled, on January 1, 2004. After that date, States will be allowed to enact laws with respect to affiliate-sharing if two conditions are met:

- The State provision explicitly states that it is intended to supplement the Federal FCRA.
- The State provision gives greater protection to consumers than is provided under the Federal FCRA.²⁶

Currently, Vermont is the only State that has a law directly regulating affiliate-sharing. Vermont law, like Federal law, allows affiliates to share transaction and experience information without any notice to a consumer and without any way for a consumer to prevent the sharing. However, before financial institutions can share credit reporting information about Vermont consumers with their affiliates under Vermont law, the institutions must obtain affirmative consent—or opt-in—from the consumer.

Because Vermont was the only State to have addressed the issue of affiliate-sharing at the time of the 1996 revisions to the FCRA, Congress specifically exempted Vermont's State consent provision from FCRA preemption "with respect to the exchange of information among persons affiliated by common ownership or common corporate control."²⁷ Congress should allow other States to address concerns with respect to affiliate-sharing by allowing the preemption of such State laws to sunset as scheduled.

Recommendations for Congressional Action

In sum, I recommend the following as appropriate steps for this Committee to take to ensure that consumers' financial privacy is protected:

1. To prevent abusive telemarketing practices of the type that led to enactment of Title V in the first instance, prohibit financial institutions from using encrypted account numbers, unique identifiers, or other means to access a consumer's account without explicit authorization from the consumer.

2. To ensure that consumers understand their rights under Federal law with respect to financial privacy, require the Federal Agencies responsible for GLB regulation to develop standard financial privacy notices similar to the nutritional labels developed by the Food and Drug Administration under the Nutritional Labeling and Education Act.

3. Ensure that consumers have effective notice and choice with respect to affiliate-sharing.

4. Continue to allow States to enact more protective provisions with respect to sharing of financial information among unaffiliated third parties.

5. Allow the preemption of more protective State laws governing affiliate-sharing to sunset as scheduled on December 31, 2003.

²⁵ See 15 U.S.C. §§ 1681t(b)(2) and (d).

²⁶ 15 U.S.C. § 1681t(d).

²⁷ 15 U.S.C. § 1681t(b)(2).

PREPARED STATEMENT OF FRED H. CATE
PROFESSOR OF LAW, INDIANA UNIVERSITY SCHOOL OF LAW
SEPTEMBER 19, 2002

My name is Fred Cate, and I am a Professor of Law and Ira C. Batman Faculty Fellow at the Indiana University School of Law in Bloomington, and a Senior Policy Advisor at the Hunton & Williams Center for Information Policy Leadership. For the past 13 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a Member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a Visiting Fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today, and I am doing so on my own behalf. My views should not be attributed to Indiana University or to any other institution or person.

The Importance of Consumer Concern

The polling data, newspaper editorial pages, this summer's referendum in North Dakota, and anecdotal evidence all suggest that consumers are concerned about personal financial information and how it is accessed and used both by the Government and private industry. It is important to view this concern in context.

The concern is not surprising, given the amount of press and political attention given privacy issues, the increased focus on privacy issues and the dramatic growth in privacy-related products and services by financial institutions, and the deluge of a billion or more privacy notices that financial institutions are required by Federal law to mail to their customers annually.

When viewed in this context, I believe the existence of consumer concern is not only predictable but largely healthy: It tells us that consumers are paying more attention to important privacy issues, and are interested in how their privacy can be better protected. Given that many of the most effective privacy protections—especially to guard against identity theft—are the steps that individuals alone can each take individually, this new interest is critical.

The Absence of Consumer Action

It is also important not to lose sight of the context of consumer action—as opposed merely to polls. Under the requirements of Gramm-Leach-Bliley, by July 1, 2001, tens of thousands of financial institutions had mailed approximately 1 billion notices. If ever consumers would respond, this would appear to be the occasion: The notices came in an avalanche that seems likely to have attracted consumer attention, the press carried a wave of stories about the notices and about State efforts to supplement Gramm-Leach-Bliley's privacy provisions, privacy advocates lauded the opt-out opportunity and offered online services that would write opt-out requests for consumers, and the information at issue—financial information—is among the most sensitive and personal to most individuals.

Yet the response rate was negligible. The available published information indicates that fewer than 5 percent of consumers responded to the deluge of notices by opting out of having their financial information shared with third parties. For many financial institutions, the response rate was lower than 1 percent. And this appears to be consistent with response rates to other privacy-related opt-out opportunities, such as the Fair Credit Reporting Act's opt-out provisions applicable to prescreening and sharing credit reports with affiliates; the Direct Marketing Association's mail, telephone, and e-mail opt-out lists; and other company-specific lists.

Before considering the adoption of new privacy laws, I would urge Congress to first consider why consumers do not take advantage of existing opportunities to restrict the sharing or use of information.

The Interference with Competing Desires

Consumers' concern about privacy protection must also be examined in the context of other consumer issues. Consumers want not only more privacy, but also lower rates on mortgages and loans, higher returns on CD's and investments, and faster and more personalized service. Privacy laws can interfere with these other objectives, both by restricting the flow of information on which they depend, and by imposing high transaction costs on consumers and financial institutions alike.

Restricting the Benefits of Open Information Flows

Consider just a few of the many examples of the consumer benefits that depend on accessible information and that are threatened by more restrictive privacy laws.

Businesses and other organizations use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: “Information about individuals’ needs and preferences is the cornerstone of any system that allocates goods and services within an economy.” The more such information is available, “the more accurately and efficiently will the economy meet those needs and preferences.”¹

Information-sharing allows financial institutions to “deliver the right products and services to the right customers, at the right time, more effectively and at lower cost,” Fred Smith, Founder and President of the Competitive Enterprise Institute, has written.² The use of personal information to recognize and respond to individual customer needs is the definition of good customer service. Personalized service—epitomized by George Bailey, small-town banker played by Jimmy Stewart in “It’s a Wonderful Life”—is what many consumers want. *The Los Angeles Times* reported in December 1999, about customers who are understandably “irritated if the bank fails to inform them that they could save money by switching to a different type of checking account.” But, of course, as the newspaper noted, “to reach such a conclusion, the bank must analyze the customer’s transactions. . . .”³

By having a complete picture of its customers’ financial situations, banks can offer them bundled services at a single lower price than if provided on an a la carte basis. Customers benefit in two ways: First, they are offered a range of diversified services that are most appropriate for their individual financial situations. Second, they get those services at a lower price.

For example, a consumer may choose to link her mortgage loan with a checking or savings account at the lender’s affiliate, and thereby avoid minimum balance requirements for the checking or savings account, and enjoy the convenience of being able to arrange for direct deductions from a bank account to make the monthly mortgage payment. A financial services institution can aggregate all of a customer’s accounts to satisfy minimum balance requirements. It can make an instant decision whether to increase a credit line, based on its total relationship with the customer. Washington attorney L. Richard Fischer writes: “Information-sharing also enables financial institutions to offer consumers popular products such as ‘affinity’ or ‘co-brand’ credit card accounts. Such programs provide frequent flyer miles, grocery, or gasoline rebates, and other benefits to credit cardholders. Other such programs permit universities and other not-for-profit organizations to benefit from cardholder use of their accounts.”⁴

To provide all of these and other opportunities, access to data is essential. Laws restricting affiliate-sharing or requiring opt-in consent make the provision of these services untenable. How could an affinity program work if the card issuer and unaffiliated partner could not share customer data? How could a lender accurately and rapidly judge the risk of increasing a customer’s credit line if it could not look at all of her accounts with affiliated companies? How would a financial services institution identify appropriate candidates for debt consolidation, if it could not examine both the range of outstanding debts and homeownership or other relevant criteria?

Information-sharing is especially critical for new and smaller businesses. By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition. Laws designed to protect privacy act as barriers to that information-sharing, and therefore, writes Robert E. Litan, Director of the Economic Studies Program and Vice President of the Brookings Institution, “raise barriers to entry by smaller, and often more innovative, firms and organizations.”⁵

The Cost of Regulation

There is also a financial cost to privacy regulation. We have already seen that a major component of that cost is caused by the interference of privacy laws with open information flows. Another source of that cost is the burden of complying with privacy laws. Crafting, printing, and mailing the billion or more disclosure notices required by Gramm-Leach-Bliley, for example, is estimated to have cost \$2–\$5 billion. Much of that cost will be repeatedly annually.

¹ Financial Privacy, Hearings before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).

² Fred L. Smith, Jr., Better to Share Information, *Desert News* (Salt Lake City, UT), October 14, 1999, at A22.

³ Edmund Sanders, Your Bank Wants to Know You, *The Los Angeles Times*, December 23, 1999, at A1.

⁴ Financial Privacy Hearings, *supra* (statement of L. Richard Fischer).

⁵ Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, Working Paper 99–3, AEL–Brookings Joint Center for Regulatory Studies (1999).

More burdensome opt-in laws, as discussed below, would prove even more costly. During its opt-in test, U.S. West found that to obtain permission to use information about its customer's calling patterns to market services to them cost between \$21 and \$34 per customer, depending on the method employed.⁶

A 2000 Ernst & Young study of financial institutions representing 30 percent of financial services industry revenues, found that financial services companies would send out three to six times more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about \$1 billion per year.⁷

The study concluded that the total annual cost to consumers of opt-in's restriction on existing information flows—precisely because of the difficulty of reaching customers—was \$17 billion for the companies studied, or \$56 billion if extrapolated to include the customers of all financial institutions. Those figures do not include the costs resulting from the reduced availability of personal information to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, and develop future innovative services and products.

These costs do not include the increased burden to consumers of additional letters, telephone calls, and e-mails seeking consent: U.S. West had to call its customers an average of 4.8 times per household just to find an adult who could consent.

The Special Problem of Opt-In

The burden of privacy laws is even greater when they forbid the use of information without affirmative, opt-in consent. While both opt-in and opt-out give consumers the same legal control about how their information is used, the two systems differ in the consequences they impose when consumers fail to act.

The U.S. Post Office reports that 52 percent of unsolicited mail in this country is discarded without ever being read. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Corporate trials of consent-based privacy systems demonstrate that no matter how good the offer or how easy the opt-in or the opt-out method, customers rarely respond.

Under opt-out, consumers like those under Gramm-Leach-Bliley who failed to read or respond to a privacy notice, still received services. Under opt-in, consumers who did not respond could not have their information used. By virtue of not responding—whatever the reason—those subject to opt-in are excluded from receiving information-dependent services. Opt-in is more costly to consumers precisely because it fails to harness the efficiency of having them reveal their own preferences as opposed to having to explicitly ask them.

For a practical, specific example of the impact of opt-in on consumers, Michael Staten, an economist, Distinguished Professor, and Director of the Credit Research Center at Georgetown University's McDonough School of Business, and I conducted a case study of MBNA Corporation, a diversified, multinational financial institution. Incorporated in 1981, and publicly-traded since 1991, by the end of 2000, the company has experienced 40 consecutive quarters of growth, provided credit cards and other loan products to 51 million consumers, had \$89 billion of loans outstanding and serviced 15 percent of all Visa/MasterCard credit card balances outstanding in the United States.⁸

The case study examined the impact of three forms of opt-in: (1) Opt-in for sharing personal information with third parties; (2) Opt-in for sharing personal information with affiliates; and (3) Opt-in for any use (other than statutorily excluded uses) of personal information.

The study found that any form of opt-in would have significant economic effects on MBNA and its customers, because of the company's extensive use of direct marketing to attract customers and its heavy reliance on personal information to identify out of the 1 billion prospect names the company receives annually from its more than 4,700 affinity groups for which MBNA issues credit cards the 400 million names of people who are likely to be both qualified for and interested in a credit card solicitation.

Given the low response rates to opt-in requests universally reflected by organizations that seek consent other than at time of service or in response to a communica-

⁶Brief for Petitioner and Interveners at 15–16, *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98–9518), cert. denied 528 U.S. 1188 (2000).

⁷Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies* 16 (December 2000).

⁸Michael E. Staten & Fred H. Cate, "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA," *Duke Law Journal* (forthcoming 2002).

tion initiated by the customer, the case study concludes that even the least restrictive opt-in regime—for third-party information-sharing—would result in the MBNA’s marketing materials being 27 percent less well targeted. As a result, 109 million people would receive solicitations who should not have. This translates into an 18 percent lower response rate and a 22 percent increase in direct mail costs per account booked. There would also be an additional 8 percent reduction in net income because of increased defaults and reduced account activity, resulting from less qualified people receiving credit card solicitations.

The broader opt-in regimes would result in more significant losses to MBNA and its customers, largely in three areas. First, MBNA’s affiliates would be unable to cross-sell services to existing customers or provide one-stop customer service, because of the restriction of sharing information across affiliates. Second, MBNA’s corporate structure, which currently includes affiliates because of tax and regulatory reasons, would be less efficient and more expensive because centralized service units would no longer be able to provide services for all of the affiliates. Third, opt-in would interfere with fraud detection and prevention efforts which depend on information-sharing across affiliates and among companies.

These costs would be incurred despite the fact that as of the end of 2000, only about 130,000 customers (one-quarter of 1 percent of MBNA’s customer base) had exercised their legal right to opt-out of having their credit report information transferred across MBNA affiliates, and approximately 1 million customers (less than 2 percent) had taken advantage of MBNA’s voluntary opt-out from receiving any type of direct mail marketing offers.

The important point is not simply that complying with privacy laws is expensive, but rather that it imposes costs on consumers. Privacy polls rarely if ever ask consumers whether they are ready to bear that cost. But ultimately, it is consumers and individuals, in the words of Alabama Attorney General Bill Pryor, who “pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace.”⁹

The Bigger Context

It is also important to evaluate consumer concerns about financial privacy in a broader context. Gramm-Leach-Bliley was passed in 1999 and the first notices were required to be mailed by July 1, 2001. Only 14 months has passed since that date, examinations of financial institutions under the new requirements are only now beginning, and enforcement has been limited. It is simply too early to judge meaningfully how well the new system is working.

Despite the short time, however, financial institutions have been busy working with Federal regulators, consumer advocates, and others attempting to improve their privacy notices and increase the effectiveness of consumer education. There was considerable criticism of the first round of Gramm-Leach-Bliley privacy notices, a key element of the law. While some of that criticism may be justified, the complexity of privacy notices seems in large part to have reflected the complexity of the law and regulations requiring them. Title V uses many terms that consumers would likely find confusing and that must be used precisely to make sense of the law’s requirements. For example, the law makes a significant distinction between “consumers” and “customers,” and this distinction was necessarily reflected in many notices, even though many people use the terms interchangeably.

It should also be noted that clarity may be in the eye of the beholder. On June 18, 2001, at a hearing on financial privacy of the California General Assembly’s Committee on Banking and Finance, the Committee Chairman challenged the financial services industry representatives in the audience to live up to the standard set by American Express’ privacy notice. In fact, he distributed to every person attending the hearing a copy of the American Express notice so that they could, in the Chairman’s words, use it as a “model.” Two weeks later, on July 9, 2001, *USA Today* editorialized in favor of clearer privacy notices, citing American Express’ notice—the same notice lauded only 2 weeks earlier—at its first example of a difficult to comprehend notice.¹⁰

As Federal Trade Commission Chairman Timothy Muris has noted, we are still learning:

The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is

⁹Bill Pryor, *Protecting Privacy: Some First Principles*, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

¹⁰“Confusing Privacy Notices Leave Consumers Exposed,” *USA Today*, July 9, 2001, at 13A.

a statute that only lawyers could love—until they found out it applied to them.¹¹

Today, regulators, industry, and consumers are learning from the emerging experience with Gramm-Leach-Bliley, and are collectively improving the quality and variety of available privacy protections. The Hunton & Williams Center for Information Policy Leadership, for example, hosts a project in which leading financial institutions are trying to develop layered notices—an approach that would make privacy disclosures easier to understand and compare. The Federal Trade Commission has hosted a workshop on effective financial privacy notices, and is working with industry and privacy rights advocates to improve notices. The Commission is also pushing forward related privacy initiatives, including a national do-not-call list and increased privacy enforcement.

Many financial services companies have also responded with privacy-related products and services, or options for individuals to control the use of their information beyond what is required by law. Many financial services companies report today that they do not share personal nonpublic financial information about their customers with third parties. Some provide opportunities for customers to opt-out of information-sharing that is expressly permitted by Gramm-Leach-Bliley. Citicorp, Capital One, Visa, and American Express all advertise credit cards offering privacy- and security-related enhancements. Bank of America and other banks are openly competing for consumer business based on how privacy protective they are. Companies are developing best practices for a variety of privacy protections; for example, Citigroup has released telemarketing best practices developed with State attorneys general.

None of these developments is likely to prove a panacea for privacy protection, but their variety and the speed with which they are being developed suggest that they will afford consumers a greater choice of privacy alternatives than any law is likely to. Most importantly, there is virtually no evidence of tangible harms to consumers that are not already covered by Gramm-Leach-Bliley, the Fair Credit Reporting Act, or some other financial privacy law.

Consumers have understandable concerns about their privacy, and some adjustments to Federal financial privacy law may eventually prove necessary. But in the absence of evidence consumers being physically or financially harmed by unregulated uses of their personal financial information, the Congress has the time to wait to see how existing laws are working and to allow market responses to more fully mature.

PREPARED STATEMENT OF JOHN C. DUGAN

PARTNER, COVINGTON & BURLING

ON BEHALF OF THE

FINANCIAL SERVICES COORDINATING COUNCIL

SEPTEMBER 19, 2002

My name is John Dugan, and I am a Partner with the law firm of Covington & Burling. I am testifying today on behalf of the Financial Services Coordinating Council (FSCC), whose members include the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. These organizations represent thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America. I have represented the FSCC on financial privacy issues since the organization was formed in late 1999, and in that capacity I have advised on implementation issues involving the privacy provisions of the Gramm-Leach-Bliley Act (GLB Act) and related regulations; participated in the Federal Trade Commission's interagency task force on notices; helped coordinate our task force devoted to improvements in privacy notices; and testified on a number of occasions before the Congress and State legislatures on GLB Act issues and various financial privacy legislative proposals.

The FSCC appreciates the opportunity to testify before this Committee on the status of financial privacy regulation, in our case from the perspective of the financial services industry. Our testimony focuses on: (1) the balance Congress struck in the Gramm-Leach-Bliley Act (GLB Act); (2) our experience with implementing the Act,

¹¹Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, 2001 Conference, Cleveland, OH, October 4, 2001.

including the reaction of our customers; (3) our views on the appropriate relationship between Federal and State privacy laws; and (4) some thoughts going forward.

The Balance Struck in the GLB Act

Every commercial privacy law strikes a balance between protecting the privacy interests of consumers *and* preserving the clear consumer benefits that arise from the free flow of information in the economy. While consumers expect limits on the disclosure of their information, they also expect companies to provide them with benefits that can only be provided through information-sharing. For example, a loyal, long-time depositor in a bank wants and expects to receive a discount on a mortgage loan offered by a related mortgage company affiliate, and such “relationship discounts” can only be provided through information-sharing. Privacy laws try to balance these competing consumer expectations.

In terms of financial privacy, we believe that Congress struck the right balance in 1999 when it adopted the privacy provisions of the GLB Act against the backdrop of the preexisting privacy protections provided by the Fair Credit Reporting Act and other Federal and State statutes. Through exceptionally broad definitions, the GLB Act’s protections apply to virtually all personal information held about the individual consumers of more than 40,000 financial institutions in this country—including less traditional “financial institutions” such as check cashers, information aggregators, and financial software providers. Coupled with protections mandated by the Fair Credit Reporting Act (FCRA), these consumers now must be provided:

- NOTICE of the institution’s practices regarding information collection and disclosure, which must be clear, conspicuous, and updated each year.
- OPT-OUT CHOICE regarding the institution’s sharing of information with non-affiliated third parties, and in certain instances, with affiliates.
- SECURITY in the form of mandatory policies, procedures, systems, and controls to ensure that personal information remains confidential.
- PROTECTION AGAINST INAPPROPRIATE REDISCLOSURE OR REUSE OF PERSONAL INFORMATION that is shared with third parties.
- ENFORCEMENT of privacy protections via the full panoply of enforcement powers of the agencies that regulate financial institutions, for example, the Federal bank regulators, the Securities and Exchange Commission, State insurance authorities, and the Federal Trade Commission.

In addition to these protections, customers of financial institutions that handle personal health information, for example, insurance companies, receive the extensive privacy protections of Federal and State medical privacy laws. Taken together, the FSCC believes that this set of provisions forms the most comprehensive set of privacy protections that has yet been implemented in the United States.

We recognize that these protections are not as restrictive as some would have wanted, including some of the witnesses on today’s panel. But by any measure, compared to 3 years ago consumers have much more meaningful information, choice, and security regarding the way that financial institutions handle their personal information.

At the same time, the GLB Act appropriately allows financial institutions to share information with others for a variety of plainly legitimate purposes without separate consumer consent, that is, to carry out transactions requested by the consumer, to deter and detect fraud, to respond to regulators and judicial process, etc. While many of these “doing business” exceptions were viewed suspiciously by critics at the time the Act was passed, they have proven to be sensible and noncontroversial provisions covering sharing for which consumer consent is simply inappropriate.

The FSCC also continues to support Congress’ decision to treat information-sharing by companies under common control in the same manner as sharing *within* a single institution; both are situations in which the GLB Act’s opt-out requirement does not apply. The fact is that many financial institutions operate through affiliated financial entities, often with very similar names, rather than through divisions of a single institution. For purposes of the opt-out, Congress sensibly elected to ignore such artificial separations and treat affiliates as part of a single organization rather than as entirely distinct entities. This decision reflected the fact that consumers are unlikely to distinguish between, for example, a community bank and the community bank’s affiliated mortgage lending company. Instead, consumers are likely to expect that both affiliates are part of a single community banking organization where information is shared within that corporate family. The decision also reflected the fact that the sharing of sensitive credit and insurance application information with affiliates is already subject to an opt-out requirement under the Fair Credit Reporting Act.

Finally, we also continue to believe that Congress made the right choice in requiring that a financial institution provide its consumers with the right to opt-out of the financial institution's sharing of the consumers' personal information with third-party commercial companies. This decision reflected the view that the sharing of personal information with such nonaffiliated third parties (other than for the exceptions described above) is different in nature than sharing information with companies within a corporate family or with financial institution marketing partners—and that it is sufficiently different from consumer expectations that a consumer should be given the choice to opt-out of such sharing.

In making this choice, however, Congress rightly rejected an *opt-in* approach, because there is a fundamental flaw with the way such requirements work. Opt-in provisions deprive consumers of benefits from information-sharing (such as the depositor's relationship discount on a mortgage loan described above), because consumers rarely exercise opt-in consent of any kind—even those consumers who would want to receive the benefits of information-sharing if they knew about them. In essence, an opt-in creates a “default rule” that stops the free flow of information. This in turn makes the provision of financial services more expensive and reduces the products and services that can be offered, which actually frustrates consumer expectations. In contrast, an opt-out gives privacy-sensitive consumers just as much choice as an opt-in, but without setting the default rule to deny benefits to consumers who are less privacy-sensitive.

Implementation of the GLB Act

The privacy provisions of Gramm-Leach-Bliley were enacted in 1999, and financial institution regulators subsequently issued detailed privacy regulations that became effective just over a year ago. This appears to be the first time that the Federal Government has implemented such a comprehensive commercial privacy regulatory regime affecting such an important sector of the Nation's economy. In a sense, financial institutions have been the “guinea pigs” for this process, and much has been learned by both the regulators and our industry.

The implementation process has been massive, involving eight Federal regulators, 51 State insurance regulators, and over 40,000 financial institutions. Companies have conducted detailed auditing of their information practices; developed and issued over 2.5 billion privacy notices; established new compliance systems; trained personnel; and reconfigured systems to handle and monitor consumer opt-outs.

Financial institutions have also upgraded their already extensive security policies, procedures, and systems to comply with the security mandates of the Act. For example, company employees with access to confidential customer information are often required to adhere to many different types of procedures designed to protect the physical security of that information, including disclosing information to other employees only on a “need to know” basis; locking confidential files and clearing desks before going home; and using special passwords to access information. In addition, some companies control access through use of security systems and computing platforms, where users are authenticated by means of logon identifications and/or secret passwords. In some cases digital certificates are also used for purposes of authentication and nonrepudiation; access control lists limit levels of access based on job employee functions; and formal data classification schemes ensure that sensitive data is stored only on secure platforms. These are just a sample of the many steps that firms are taking in the security area.

In short, while tremendous progress has been made, GLB implementation is still very much a work in progress, and financial institutions continue to learn, adjust, and improve their privacy and security practices over time. One thing is certain, however: As the result of the Gramm-Leach-Bliley's notice, choice, and security requirements, financial institution customers are far more privacy and security-protected than they were 3 years ago, and far more protected than the customers of most other types of companies. We believe that consumers have responded favorably by continuing to put their trust in the companies that handle their financial assets and their financial needs.

Indeed, despite generic polls showing that consumers remain concerned about their privacy, financial institutions have received a minuscule number of customer complaints about the GLB Act procedures or other privacy concerns. The same is true of financial regulators. For example, in response to a Freedom of Information Act request regarding all financial institution complaints received in 2001, the Federal Reserve reported that it had received only 25 privacy-related complaints out of the 4,503 complaints it received, or .0056 percent of the total, with similarly low numbers reported by the Office of Thrift Supervision (6 of 4,921, or .0012 percent), Federal Deposit Insurance Corporation (137 of 6,849, or .02 percent), and Office of the Comptroller of the Currency (368 of 17,228, or .0214 percent).

In addition, most financial institutions do not share information with third parties, such as commercial companies, in a way that triggers the need for the GLB Act opt-out requirement. For example, roughly 89 percent of a recent sample of approximately 400 banks conducted by the American Bankers Association did not share information in this way. For those institutions that do share with third parties in a way that requires providing the opt-out to consumers, the opt-out rates have generally been low, and in nearly all cases under 10 percent. The FSCC strongly disagrees with those who suggest that low opt-out rates mean that the GLB process is not working. To the contrary, our members believe that the low rates show that consumers trust their financial institutions to share their information in an appropriate manner, or that they are less sensitive to privacy concerns than has been suggested.

Based on initial implementation experience, the FSCC recognizes that the privacy notices constitute one area in which improvements can be made. This is by no means as easy as it sounds, however, because the notice requirements of the GLB Act are quite detailed. The financial institution regulators tried hard to simplify these requirements in their implementing regulations, including through the use of sample clauses, and they told institutions that a notice complying with the GLB Act could fit on a six-page, "tri-fold" brochure. In their first round of notices, financial institutions generally took this approach and used the sample clauses, while at the same time carefully scrubbing the language to ensure compliance will all requirements of the statute and regulations.

Proceeding this way was absolutely necessary to ensure that the notices satisfied the regulators' "clear and conspicuous" requirement and minimized exposure to legal liability. Indeed, the regulators have challenged very few privacy notices as failing to comply. Nevertheless, a six-page notice is not short, and language from the sample clauses such as "nonaffiliated third-party" and "nonpublic personal information" are obviously the type of "legalese" that some consumers and critics have found difficult to understand.

Unfortunately, financial institutions now find themselves in a bit of a "Catch-22." They spent hundreds of millions of dollars to carefully develop the first round of compliant notices and mail them to consumers, and financial institution consumers received more information about company privacy practices than consumers of virtually any other industry in the country. Yet these very same notices, because of their length and use of legalistic terms suggested by the regulations, have received a great deal of negative attention in the media.

To address these concerns, the financial services industry is proceeding down two paths simultaneously. First, a number of institutions have simplified the language used in their second round of annual privacy notices, though carefully so as not to stray from the requirements of the regulation. We believe the second round of notices will be more "user friendly" than the initial notices.

Second, both financial institutions and their regulators have focused on the idea of exploring a simplified "short-form" version of the notice that would supplement, but not replace, the longer "legal notice" required by the GLB Act and regulations. The FTC convened an interagency and industry workshop to discuss this and other notice issues, and industry efforts are underway to examine the short-form concept more carefully. The basic idea of the short-form notice is to use simplified terms, be much less legalistic than the longer notice, keep the length to one page, and use common language that would make it easier for consumers to compare institution privacy policies over time.

The FSCC is leading a project on the short-form notice. We have convened a task force representing a cross-section of institutions from the banking, insurance, and securities industries; hired a well-known language expert to advise on short-form issues; and have nearly completed the initial drafting phase of several possible alternatives.

While we believe this project is promising, it is by no means simple, as I mentioned previously. There is no true "one-size-fits-all" solution, because institutions have different privacy practices that call for different types of disclosures.

Relation Between Federal and State Privacy Laws

There seems to be a great deal of misunderstanding about Gramm-Leach-Bliley's effect on State privacy laws, as well as on the amount of State legislative action that has occurred on financial privacy issues generally. On the first point, Section 507 of the GLB Act makes clear that its privacy provisions would not preempt any State law in effect simply because the State law affords greater privacy protections to consumers than the Act's provisions. Of course, this provision by its terms does nothing to limit the preemptive effect of any other Federal statute, specifically in-

cluding the Fair Credit Reporting Act's preemption provision that applies to State law restrictions on affiliate information-sharing.

Some State legislators seemed to interpret Section 507 as an affirmative invitation by the Federal Government to the States to adopt more restrictive financial privacy laws than Gramm-Leach-Bliley. This interpretation spawned a great deal of State legislative interest in new financial privacy laws immediately after passage of the GLB Act in 1999. The FSCC and numerous other representatives disagreed with that interpretation and testified to that effect before a number of State legislatures. Our position consistently has been that there was no such Federal invitation for States to act in Gramm-Leach-Bliley; that States should *not* rush to act before the GLB Act has been fully implemented and given a chance to work; and that a patchwork, uneven body of differing State privacy regulation would be extremely costly and counterproductive. In short, we believe that a single uniform standard in Federal law is the most appropriate method for regulating financial privacy.

This leads me to the second point of confusion. While there has been a flurry of activity and debate at the State level in the wake of passage of the GLB Act in 1999, during this period no State legislature has adopted a comprehensive financial privacy statute that has exceeded the obligations of the GLB Act. Nearly 40 States considered such privacy legislation in 2000, but no such statute was enacted. About half that number revisited the issue in 2001, again without final action. And this year, only California has come close to enacting a new privacy law, but for the third time in 3 years, the legislature has chosen not to act.

We recognize that North Dakota first chose to conform a preexisting bank privacy opt-in law to the limits of Gramm-Leach-Bliley, only to have an initiative restore the preexisting law. In addition, regulators (but not legislatures) in New Mexico and Vermont have issued additional financial privacy regulations (though the Vermont legislature had earlier rejected an effort to increase financial privacy restrictions, and a lawsuit has been filed to challenge the Vermont regulation as beyond the scope of Vermont statutory authority). *But taken together, these few actions simply do not constitute a groundswell of State action to impose more restrictive financial privacy regulation.*

To the contrary, with the notable exception of California, the State focus on financial privacy legislation has diminished considerably over time since the GLB Act was enacted. The FSCC believes this is due in large part to an increased understanding that: (1) The Gramm-Leach-Bliley protections are substantial and need to be given a chance to work before States decide to act further; and (2) it is not nearly as easy as it seems at first blush to adopt financial privacy restrictions without causing unintended consequences that increase costs and deprive consumers of real benefits.

Actions in the Future

The Gramm-Leach-Bliley's privacy protections are real, and the implementation, adjustment, and enforcement process is ongoing. This is not to say that improvements cannot be made, however. In particular, the FSCC believes that the process for improving privacy notices is well worthwhile, and we plan to pursue that process actively in the coming months, both within the industry and with our regulators.

In terms of Federal legislation, we believe that any additional action that Congress considers with respect to privacy issues should be targeted to specific harms rather than take the form of sweeping data protection restrictions. If the harm to consumers is identity theft, then the focus of legislation should be on deterring and remedying that problem specifically. Similarly, if consumers are most concerned about excessive telemarketing calls resulting from information-sharing, then we believe that solutions should address that issue specifically. To do otherwise by imposing broad restrictions on information use and sharing: (1) May do little to solve the specific harms at issue; and (2) may have very negative unintended consequences. Accordingly, the FSCC stands ready to work with this Committee and other public policymakers to address specific consumer harms.

In this regard, however, the FSCC could not support any new financial privacy legislation that did not include Federal preemption to ensure a uniform national privacy standard. The FSCC has similar concerns with respect to the FCRA provision that preempts State restrictions on affiliate-sharing, but is scheduled to sunset by the end of 2003. The FSCC supports extending the sunset, as we believe that the uniform national affiliate-sharing provision has allowed financial institutions to serve their customers in the most efficient manner possible.

Thank you for allowing me to present the views of the FSCC today. I would be happy to answer any questions.

PREPARED STATEMENT OF MIKE HATCH*

ATTORNEY GENERAL, STATE OF MINNESOTA

SEPTEMBER 19, 2002

I appreciate the opportunity to address the Senate Committee on Banking, Housing, and Urban Affairs on the critical issue of protecting the privacy of our citizens' financial information. This Committee has taken a leading role in the challenge to protect consumer financial privacy. I commend the bipartisan efforts of Senators Sarbanes and Shelby in addressing these issues.

Unfortunately, Title V of the Gramm-Leach-Bliley Act (GLBA) is not working to protect consumers from the misuse of their financial information. The Act has confused consumers, provided a green light to the unauthorized sharing of personal financial data as part of misleading telemarketing campaigns, and is riddled with loopholes that exempt many business practices from any control. I will focus my remarks on three aspects of GLBA: (1) The opt-out provisions in Section 502(b); (2) the limitations on sharing of account numbers in Section 502(d); and (3) the favorable preemption standard in the Sarbanes Amendment, Section 507. While the alleged consumer "protections" in Section 502 have proven of limited value in protecting consumers, Section 507 is an important part of GLBA that may ultimately provide various State models for how to more fairly balance the needs of business with the privacy rights of consumers.

Opt-Out Is Ineffective To Protect Consumers

The opt-out system is not an effective means of protecting consumer financial privacy. It puts the burden on consumers to look for the privacy notices, read and attempt to understand them, and then take affirmative action to halt the sharing of their nonpublic personal information with nonaffiliated third parties, such as telemarketers. This system is contrary to how consumers act in the marketplace and what consumers expect from Government efforts to remedy the imbalance of power in the marketplace. Businesses that want to share personal financial information should do no more and no less than is required in any consumer transaction—obtain prior express consent of the consumer; in other words, opt-in to the deal.

The current system does more to confuse than to assist consumers. The opt-out notices flooding consumers' mailboxes have been a boon for the printing and postal industry, but they have not meant much for the typical consumer. The notices are dense and impenetrable. Even the most educated and persistent of consumers would have a hard time deciphering statements such as "we may disclose [information to] . . . carefully selected business partners (that is, so they can alert you to valuable products and services)"¹ to mean the financial institution will allow telemarketers to charge your credit card account without obtaining a signature or account number from you. The ineffectiveness of the notice and opt-out procedure has been thoroughly documented.²

GLBA Limitations On Account Number Sharing Have Had No Meaningful Impact On Preacquired Account Telemarketing Abuses

Each year, American consumers experience millions of dollars of unauthorized charges on bank, credit card, mortgage, and other accounts as a direct result of financial institutions sharing personal financial data. Despite an attempt at appearing to address this concern, GLBA has had no effect on the problem. In fact, GLBA may have inadvertently acted to legitimize financial institutions' participation in data-sharing practices that result in deceptive telemarketing practices.

Preacquired Account Telemarketing Abuses

Financial institutions sell to telemarketers the names, phone numbers, and other information about their customers along with the right to charge the accounts of those customers. Telemarketers use this charging authority to call consumers with a "free trial" or "no risk" offer for services like travel membership clubs and credit card protection insurance. The telemarketer, because it has the ability to directly charge the account, never obtains an account number, a signature, or any other traditional evidence of consent from the customer. This sales practice, known as

*All Exhibits held in Committee files.

¹See <http://www.capitalone.com/index.nhp>.

²See Mark Hochhauser, Ph.D., *Lost in Fine Print II: Readability of Financial Privacy Notices*, Privacy Rights Clearinghouse, May 2001, available at <http://www.privacyrights.org/ar/GLB-Reading.htm>. The eight Federal agencies that issued regulations implementing GLBA held a workshop in December 2001, that also documented consumer misunderstanding and noncomprehension of the notices. See <http://www.ftc.gov/bcp/workshops/glb/index.html>.

preacquired account telemarketing, has led to a constant and heavy flow of complaints to Attorneys General and other consumer protection agencies.

Preacquired account telemarketing is inherently unfair and causes deception and abuse, especially with elderly and vulnerable consumers. This sales practice turns on its head the normal procedures for obtaining consumer consent. Other than for a cash purchase, providing a signature or an account number is a readily recognizable means for a consumer to signal assent to a deal. Decades of consumer education have made many consumers aware that disclosing their account number may result in unexpected charges. The corollary to this is that many consumers believe that as long as they do not disclose their account number, no charge can be made on the account. Preacquired account telemarketing exploits this belief.

When financial institutions share with the telemarketer the information needed to directly charge a customer's account, it removes these short-hand methods of consumer control over consent to a purchase. Preacquired account telemarketing strips the consumer of control over the transaction and exploits the belief that being careful about disclosing an account number provides protection. The telemarketer not only establishes the method by which the consumer will provide consent, but also decides whether the consumer actually consented.

Our Office has brought a series of cases exposing this practice.³ Fleet Mortgage Corporation, for instance, entered into contracts in which it agreed to charge its customer-homeowners for membership programs and insurance policies sold using preacquired account information. If the telemarketer told Fleet that the homeowner had consented to the deal, Fleet added the payment to the homeowner's mortgage account. Angry homeowners who discovered the hidden charges on their mortgage account called Fleet in large numbers.⁴ A survey taken by Fleet of its customer service representatives is attached as Exhibit A. It showed that customers overwhelmingly told Fleet that they did not sign up for the product, and wanted to know how it was added to their mortgage accounts without their approval, consent, or signature. Fleet's employees shared the resentment of these consumers, with comments such as "unethical for Fleet to add [optional insurance] without my permission;" "[homeowner] knows they are being slammed w/ ins they never authorized (and) thinks unethical & bad business by us . . . I agree with the customer;" and "they feel this is fraud. . . . It is a scam."⁵

The number of financial institution customers affected by this sales practice is staggering. An investigation of a subsidiary of one of the Nation's largest banks revealed an extraordinary number of complaints of unauthorized charges. During a 13 month period, this bank processed 173,543 cancellations of membership clubs and insurance policies sold by preacquired account sellers. Of this number of cancellations, 95,573, or 55 percent, of the consumers stated "unauthorized bill" as the reason for the request to remove the charge.⁶

The frail elderly, consumers who speak English as a second language, and other vulnerable groups are especially at risk with preacquired account telemarketers. A review of randomly selected sales of one preacquired account telemarketer investigated by our Office showed 58 percent of customers whose accounts were charged were over 60. Sellers continually use preacquired account telemarketing to sell elderly consumers membership clubs, magazines, and other products for which they have no possible use. Examples from our Office's investigations of telemarketers using preacquired billing information include the following: Charges to the credit card of an 85-year old man with Alzheimer's; charges to the credit card of a 90-year old woman who asked to "quit this" and said "sounds like a scam to me;" charges

³*State of Minnesota v. U.S. Bancorp, Inc.*, Case No. 99-872 (Consent Judgment, D. Minn. 1999); *In The Matter of Damark International, Inc.*, Case No. C8-99-1038 (Assurance of Discontinuance, Damsey Cty. Ct. 1999); *State of Minnesota v. Memberworks, Inc.*, Case No. MC99-010056 (Consent Judgment, Hennepin Cty. Dis. Ct. 2000); *State of Minnesota v. Fleet Mortgage Corporation*, 158 F.Supp.2d 962 and 181 F.Supp.2d 995 (D. Minn. 2001) (Consent Judgment, D. Minn. 2002).

⁴Approximately one-fifth of all calls by Fleet customers were about these preacquired account charges. The mortgage statements issued by Fleet hid the charges under the rubric "opt.prod." (optional product) at the very bottom of the bill in small print, such that it was extremely difficult to discover the charge or discern the purpose of the charge. For consumers on auto-draft from their checking or other bank account, Fleet gave no written notice of the charge.

⁵As a result of a settlement of our Office's case against Fleet Mortgage Corporation, its customers were given the opportunity to request a refund of charges for membership programs sold through preacquired account telemarketing. Over 72 percent of the customers *currently being charged* for such a program returned a form requiring a refund of charges, stated that they did not authorize the charge, and asked to have the program cancelled.

⁶The other primary reason given for cancelling (by 56,794 customers, or 32 percent of the total) was a general "request to cancel" code that may have also included many consumers claiming unauthorized charges.

to the credit card account of an Hispanic man who says “no se es” in response to a telemarketer’s question; and charges to the bank checking account of an impaired 90-year old man who did not believe he consented to the charge. Attached as Exhibit B is a letter from a Legal Aid attorney listing a variety of useless and expensive membership clubs charged to the credit card of a retired church janitor in his late 80’s. The janitor was charged for a home protection plan even though he lived in a nursing home; an auto club membership even though he had no car; a dental plan even though he already had coverage; and a credit card security plan even though Federal law already protected him from theft of a credit card.

These are just a few of the substantial number of consumer complaints our Offices have received about this sales practice. In fact, this Office receives as many complaints about these practices post-GLB as it did before enactment of the law.

GLBA Has Had No Impact On Preacquired Account Telemarketing Abuses

GLBA has not changed the involvement of financial institutions in preacquired account telemarketing, and the abuses continue to occur. All 50 State Attorneys General recently filed comments with the Federal Trade Commission (FTC) stating that consumer complaints and State consumer protection enforcement actions against preacquired account telemarketers have continued without significant change after passage of the GLBA. The reason is not hard to discern.

GLBA, in Section 502(d), prohibits a financial institution from disclosing, “other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third-party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.” Thus, Section 502(d) prohibits the practice by financial institutions of providing the credit card numbers of its customers to nonaffiliated third-party telemarketers. When sellers of magazines, membership clubs, insurance programs, and other services solicited the financial institutions’ customers via telemarketing calls, the customers were never asked to recite their credit card numbers because the sellers already had the numbers on hand with the capability to send through a charge.

After Section 502(d) of GLBA was enacted, however, the Federal banking agencies promulgated rules that permitted financial institutions to continue sharing account numbers with third-party sellers as long as they were in encrypted form. As a result of this Rule, the practices of financial institutions and their third-party sellers have remained the same. Financial institutions may share encrypted or randomly generated reference numbers for their customer’s accounts with third-party sellers. These sellers can still send through charges to consumers’ accounts without consumers giving their credit card numbers. The encrypted numbers are simply decrypted by the financial institution and the charges are put directly on the consumer’s account. This allows preacquired account telemarketing process to continue—legally and unimpeded. Unscrupulous telemarketers can still cause a charge to a consumer’s account even when a consumer says “no” to the sale, or simply believes he or she is trying out a free trial offer.

The essential characteristic of preacquired account telemarketing is the ability of the telemarketer to charge the consumer’s account without traditional forms of consent—for example, paying cash, providing a signature, or providing a credit card or bank account number. The key is how the agreement between a company controlling access to a consumer’s account and the telemarketer who preacquires the ability to charge a consumer’s account affects the bargaining power between that telemarketer and the consumer. GLBA, as interpreted in implementing regulations, does not address this relationship.

GLBA’s Favorable Preemption Language Is Critical To Future Consumer Privacy Protections

Although Title V of GLBA has done little to address the privacy needs of financial institution customers, the Sarbanes Amendment, Section 507, offers the best hope to secure protections for consumers. It is imperative that GLBA retain favorable preemption standards for State legislation.

State legislatures have taken or considered a variety of approaches to protecting consumer information. North Dakota voters recently reinstated an opt-in approach to consumer financial information that had previously been in effect. California’s legislature has alternately passed and seriously considered various consumer privacy initiatives. The Minnesota Senate has passed an opt-in financial privacy bill.

State privacy initiatives have been the subject of enormous industry legislative pressure. In an article entitled, “Lobbyists Swarm to Stop Tough Privacy Bills in States,” *The Wall Street Journal* reported on the “regimented lobbying forces of the

Old Economy” that have opposed such measure.⁷ Despite this intense effort, State privacy bills continue to advance in State legislatures. Proposed revisions to GLBA that would preempt such State action would be the death knell for meaningful reforms to protect consumers against misuse of their personal financial information.

Conclusion

I thank the Committee for its consideration. Consumer protection efforts in the area of financial privacy are in a beginning stage of development. Title V of GLBA has not adequately protected the privacy of the average citizen. I hope that the Congress will support the continuation of State legislative efforts at meaningful reform of our privacy laws.

PREPARED STATEMENT OF JAMES M. KASPER REPRESENTATIVE NORTH DAKOTA HOUSE OF REPRESENTATIVES

SEPTEMBER 19, 2002

Chairman Sarbanes and Members of the Senate Committee on Banking, Housing, and Urban Affairs. Thank you for the opportunity to share my views on financial privacy and consumer protection.

Background

I am a first term member of the North Dakota House of Representatives and I am considered a conservative in my State of North Dakota. I have been active in political affairs for over 20 years in North Dakota. I believe I bring a unique perspective to the financial privacy issues as my business career is in the financial services industry. I am an independent licensed insurance and securities broker, and my practice is in the area of employee benefits plans and business insurance planning. My entire career has been spent in Fargo, North Dakota, with the exception of 1 year in Minneapolis, Minnesota. Because North Dakota law has allowed banks to sell insurance for many years, I have competed with banks this entire time, and have a very good understanding of how they compete and what their marketing practices are.

My First Legislative Term—2001

Little did I realize that in my first Legislative session, beginning in January of 2001, a great deal of my time would be spent attempting to stop North Dakota banks from changing the very protective financial privacy law that North Dakota has had in effect since 1985. North Dakota privacy law protects not only consumer transactions, but all business and commercial transactions as well. *Our bank privacy law, enacted in 1985, prohibited the sharing and sale of consumer information to anyone, affiliates and nonaffiliates, for any reason.* In today's vernacular, we had a No-Opt for affiliates and a No-Opt for nonaffiliates. In 1997, the banking lobbyists quietly amended ND law to allow affiliate-sharing of information, so the banks in ND could legally share confidential information with their affiliates, without consent. Many citizens feel this needs to be addressed in our 2003 Legislative Session.

National Strategy of Banking Industry

As you know, the Gramm-Leach-Bliley Act (GLB) was passed by the Congress, with an implementation date for Title V of GLB of July 1, 2001. GLB deregulated the financial services industry and allows banks, insurance companies, and securities companies to have common ownership and to market each other's products. It is my understanding that two organizations, the Financial Roundtable and the Financial Services Coordinating Council, have targeted all States that have a more protective privacy law than the minimum requirements of GLB, to eliminate those States' privacy laws. They seem to be determined to stop any State Legislature from enacting any privacy laws that are more protective of consumer privacy than GLB and also to repeal any State privacy laws that are more protective than GLB.

ND Banks Work to Repeal ND Privacy Law in 2001 Legislative Session

To accomplish the bankers national goals required the repeal of our 1985 North Dakota privacy law. Therefore, the North Dakota Bankers Association, the North Dakota Independent Bankers Association and the North Dakota Credit Union Association had Senate Bill 2191 (SB 2191) introduced in the North Dakota Senate. This

⁷Zimmerman, R. and Simpson, G., "Lobbyists Swarm to Stop Tough Privacy Bills in States," *The Wall Street Journal* (April 21, 2000).

bill's intent was to repeal our 1985 North Dakota privacy law, and replace it with the GLB definitions of privacy, thus reducing ND citizen's privacy protections.

Senate Bill 2191 passed the ND Senate, in February 2001, and was assigned to the House of Representatives Industry, Business, and Labor Committee, of which I am a member. When I became aware of the intent of SB 2191, I made the decision to work to kill the bill. For 30 years, I have competed against the banks in ND and I have seen how they use credit leverage to obtain sales and to eliminate competition. I had also learned how people's personal and confidential financial information is being gathered all over the country, fed into huge computer data bases, and how consumer profiles of the citizens of our Nation are developed and sold to telemarketing companies. I believe these practices need to be stopped. I also believe they may be unconstitutional.

The banks focused all of their power in the ND House to pass SB 2191. They had 3 full-time lobbyists at the capitol for about 6 consecutive weeks. The Credit Unions had two full-time lobbyists. Additionally, representatives of Wells Fargo, U.S. Bank, and other large banks, made numerous visits to most of the Legislators and almost every one of the Legislators had personal visits from their local bankers. All of these lobbyists were urging the Legislators to support SB 2191. Their reasons were quite interesting:

The Banks and Credit Unions Used the Following Arguments in Support of SB 2191 in North Dakota:

- *"North Dakota needs to pass SB 2191 to adopt GLB in North Dakota law, so we will be in compliance with GLB."* We know this is not correct, because GLB is the law in all States, but does specifically allow State privacy law to supercede GLB, if the State law provides greater privacy protection for consumers than GLB.
- *"North Dakota will experience job loss, if we do not pass SB 2191."* Many of us believe the opposite is true. Because ND privacy law provides protection for all financial transactions, including businesses, ND could actually attract business and gain jobs, due to our privacy laws.
- *"North Dakota will experience negative economic development if we do not pass SB 2191. Businesses won't want to come to ND if we do not have the GLB privacy definitions in our law. It will be too expensive and too onerous to do business in ND."* Again, this argument was not correct. If a business does not have to waste its time to Opt-Out, business expenses are reduced. With a No-Opt law, a business will not need to use any of its resources to track its privacy records, because there are none to track.
- *"We do not want North Dakota to be the only State in the Nation, an 'island,' which has different privacy laws than the other States."* Again, an untrue argument. I believe there are 5 States that have more protective privacy laws than GLB; Alaska, Connecticut, Illinois, Maryland, and Vermont.
- *"If we do not pass SB 2191, the people of North Dakota may not be able to use their ATM, credit cards, and their checking accounts."* Since June 11, 2002, when the people of ND repealed SB 2191, our ATM's, credit cards, and checking accounts are working just fine, as they have since 1985, when we first passed our privacy law.

All of these scare tactics and more were part of a carefully orchestrated campaign by the ND banks, in conjunction with their national associations, to confuse the issues at best, and out and out lie to the Legislators at worst, about the truth of SB 2191.

There were just a handful of Legislators that worked to stop this onslaught by the Bankers and Credit Unions. The final vote in the ND House, was 77 to 20 to pass SB 2191. The ND Senate voted by 34 to 12 to pass SB 2191. The Governor, a former banker, signed the bill and it became North Dakota law on July 1, 2001.

The Referral of SB 2191—The People of North Dakota Speak

Fortunately, this was not the end of the story. In early July 2001, a small group of ordinary citizens formed a group to repeal SB 2191. They called themselves "Protect Our Privacy." In North Dakota, the people are allowed to refer any act of the Legislature by gathering the minimum amount of signatures on petitions. In about 6 weeks volunteers gathered over 17,000 signatures, about 2.5 percent of our States population, far exceeding the minimum needed to refer SB 2191. The people of ND would now vote on the referral on June 11, 2002, to decide if they wanted to repeal SB 2191. That meant we had about 10 months before the referral vote. During this time the banks organized, hired an advertising agency, and raised big money to fight the referral. They even hired two incumbent North Dakota Legislators to be

the co-chairs of their committee, which they ironically named “Citizens for North Dakota’s Future.”

Grass Roots Organization: “Protect Our Privacy” to Repeal SB 2191

The grass roots organization against SB 2191 “Protect Our Privacy,” had no money and no paid staff. All we had was a small group of committed volunteers, who like Winston Churchill, were determined we would “Never, Never, Never, Never Give Up.”

To counter the power and money of the big banks, we wrote letters to the editor, appeared as guests on radio talk shows, held press conferences, and made appearances before civic groups. About 2 weeks before the vote on June 11, 2002, we obtained a contribution of \$25,000 from the National ACLU, which allowed some radio spots to be run the last 10 days before the vote. Prairie Public Television also hosted a half hour debate about 2 weeks before the vote. Other than this, the campaign to repeal SB 2191 was by word of mouth, truly grass roots. Mr. Chairman, I would like to provide the Committee with copies of relevant documents for the record, concerning these matters.

Big Bank Media Campaign to Keep SB 2191 Backfires

All of this was small in comparison to the huge amounts of money the big banks spent on their advertising. Their media campaign was overwhelming in ND. Radio, TV, newspapers, talk shows, and civic presentations, began statewide. They obtained endorsement from our State Chamber of Commerce, from our former popular Governor, and most of the local Chambers of Commerce in our major cities. They even pirated the “Protect Our Privacy” group’s name, adopting and registering the slogan, “Protect Your Privacy” and used it on their literature to further attempt to confuse ND voters. The various banks and credit unions placed pamphlets and brochures in their customers checking and savings statements and they placed signs in many lobbies, encouraging a yes vote on SB 2191.

In their most memorable TV ad, they actually showed a wall being built around North Dakota, stating that we would become an island if SB 2191 was repealed. The one thing the bankers would not talk about, however, was the truth about SB 2191. The banks want unlimited access to and the ability to sell and share their customers’ personal and confidential financial information, without the customers’ consent or knowledge. The Opt-Out notices required by GLB, which are supposed to be privacy notices and are supposed to provide consumers with an opportunity to stop the banks from sharing information, are a joke. Statistics indicate that over 95 percent of the people of our country throw these notices away because they: (1) Do not understand them; (2) do not realize their importance; and (3) do not know the ramifications of not sending them back to the financial institution.

The Vote in North Dakota—June 11, 2002

The people of North Dakota spoke loudly and clearly on June 11, 2002, when by a 73 percent vote, they threw out and repealed SB 2191 and thus returned North Dakota privacy law to our very protective privacy statutes. Despite being out-spent 10 to 1, despite the bankers deliberate attempt to confuse the issues with their media campaign and despite the power of the banks and their hired staff, the people of ND saw through the charade of SB 2191. Their message is a national message for the Congress as well.

The Message to the Congress from the People of ND by Their June 11, 2002

Vote on Privacy is:

- Give us back and protect our privacy.
- Our financial and personal information is ours. It does not belong to the banks and other financial service companies, or anyone else for that matter. It is not for sale.
- If we want to purchase a financial product, we are very capable of initiating the call or contact ourselves.
- We are not waiting breathlessly at home for our phone to ring, to be solicited by someone with the latest, greatest product, financial or otherwise, that we just cannot do without.
- We want our identity protected.
- Our financial and personal information is a property right we believe is protected under the U.S. Constitution.
- A bank should have no more right to sell my information than it does to enter my property, steal my car and sell it without my consent.

Why Do Banks Need Unlimited Access to People's Financial and Personal Information?

It is all about market share, profit, and corporate greed, just like what our Nation has recently experienced with the Enron scandal, wherein too many corporate executives will do anything to make profits and gain market share.

The lifeblood needed to increase market share by the Financial Services companies is the free flowing and easy access to consumers' personal and confidential financial information. The GLB Act does not result in fair, open and more competition in the financial services industries. It results in the elimination of competition, wherein the big get bigger and small businesses by the thousands and hundreds of thousands will eventually be driven out of business, because they cannot compete with the financial might of the Citicorps and other mega financial conglomerates. GLB will have a long-term negative impact on rural America, as well. In ND, our State Legislature spends millions of dollars to attract new businesses to relocate to our State and our rural areas. Yet, we have a Federal Law, GLB, which places small businesses at a tremendous competitive disadvantage. When jobs disappear, the people leave. We are already experiencing this result all over America today.

Example of How Banks Share Information

My best client is a small business in Fargo, North Dakota. I have handled their insurance needs for almost 20 years. When they have an insurance need they call me. Recently, one of the principals called and asked me to come to his office to look at a life insurance proposal they had just received from their big bank insurance agent. This agent had been given their corporate and personal financial information, including salaries, ownership percentages, ages, tax bracket, Social Security numbers, dates of birth, and additional confidential information, without their consent or knowledge. They had never met or heard of the insurance agent and they had not asked for any insurance proposals. My clients were astonished and upset that the bank gave this insurance agent their information without their consent or knowledge.

My Mother's Financial Needs

My mother, who is a 79-year-old widow, just had a CD come due at her local bank, worth about \$14,500. When discussing the CD renewal with the bank teller, she was told she should look at transferring the CD to an annuity. We learned later the bank teller was not licensed to sell annuities and did not know a thing about the rest of my mother's financial affairs. She just advised her to buy an annuity from the bank.

The bank teller had no knowledge of my mother's financial needs, other than the fact she had a CD due. Despite this fact, a financial recommendation was made to purchase an insurance product from someone who was not licensed and had no idea what the impact would be on my mother's overall needs.

These are two examples of what goes on literally thousands of times every day.

A California Trip in July 2002—Bank Tactics the Same Everywhere

Senator Jackie Speier, (D) California, invited me to come to Sacramento to help move forward her privacy bill, which was in trouble in the California Assembly (House of Representatives). I spent 4 days in CA in early July 2002, a few weeks after the repeal of the SB 2191 in North Dakota. I found the big banks were using the identical tactics in CA as they had in ND. One of their tactics was to confuse the issues. They also used intense lobbying pressure from banking representatives. Unfortunately, their tactics worked, as Senator Speier's bill was just recently defeated by a few votes. As I stated earlier, there appears to be a national strategy by the Banking Industry, to kill all attempts by State Legislatures to enact any State Legislation that is more protective than the GLB privacy rules. It worked again in California.

Where Should Congress and the Senate Banking Committee Go from Here

It is imperative, in my opinion, that this Committee draft amendments to Title V of GLB, to do the following:

For nonaffiliate transactions, enact a No-Opt provision, prohibiting the sharing and selling of personal and financial information to nonaffiliated third parties for any reason, with the exception of data processing for customer requested transactions such as ATM's etc., and for transactions required by law to comply with Federal and State statutes.

Amend GLB to provide for an Opt-In method of privacy protection for all affiliates-sharing and selling of information. The people of our Nation should have the

right to stop their information from being passed around, to affiliated companies, and it should only be allowed with their advanced written consent and knowledge.

Repeal the Joint Marketing loophole. This charade of an exemption makes a mockery of the already weak privacy protections in current GLB, as almost any transaction can be designed by the banks to be exempt under this part of GLB.

Enact Legislation to provide privacy protections for all financial transactions from all sources, including business, agriculture, and nonprofit financial transactions. Under GLB these types of entities have no privacy protection whatsoever. They should have the same privacy protections that consumers do.

What Will Happen if Congress Fails to Amend GLB?

The people of the United States and the Legislators of the State Legislatures are beginning to realize the damage that has been done to the people of our country over the past number of years, due to the free flowing and public availability of their private and confidential information. I know of three States where Legislators are currently working on State Legislation to override the GLB privacy rules and to enact State Legislation similar to North Dakota's recently restored privacy law. I believe this is just the beginning of what will become a national ground swell, wherein the State Legislatures will enact real privacy protection for their citizens. Congress should act immediately to correct the mistakes made in GLB and change its privacy provisions, as suggested in this testimony.

California Initiative—2004 Vote

Due to the failure of the CA Legislature to pass Senator Speier's privacy law in California, an initiated measure has begun, headed by Chris Larsen, Chairman and CEO of e-Loan.com an Internet mortgage loan company. I predict it will be overwhelmingly successful in 2004, regardless of how much money the big banks spend to defeat it. In fact, the more they spend, the larger the vote will be to pass the privacy law in CA, because the banks cannot address the truth about how they use people's private and confidential information. It is their dirty little secret, their Achilles heal. They want to be able to sell it and share it without the people's knowledge or consent, but they cannot talk about it truthfully and openly, because they know their customers are overwhelmingly against this practice.

The Real Tragedy Perpetrated on the American People

I believe that the Congress needs to realize the damage and danger they have perpetrated on the American people by failing to pass real privacy protection. What has been done under GLB and its sister law, the Fair Credit Reporting Act, is to make people's private information a public commodity, available to all those who have the money to buy it. By allowing the privacy protections of the people of our Nation to continually be eroded, traded, and sold as just another commodity, the very fabric of our Republic is threatened. When our citizens no longer feel safe and secure in their homes and in the workplace, because their most personal and private information is no longer personal and private, we face the very real possibility that our citizens will lose confidence in our financial services industries. If that occurs, we will be in tremendous trouble. If you do not think it can happen today, all you need do is look back to 1929 and what occurred in our Nation then. Those who do not remember history are bound to repeat it.

Strong and meaningful amendments are necessary now to strengthen the Federal privacy law in GLB. I urge this Committee to courageously move forward to do so.

Thank you, Mr. Chairman, and all of the Committee Members, for the opportunity to share my experiences and viewpoints with you today. It has been an honor.

PREPARED STATEMENT OF PHYLLIS SCHLAFLY

PRESIDENT, EAGLE FORUM

SEPTEMBER 19, 2002

Totalitarian governments keep their subjects under constant surveillance by requiring everyone to carry "papers" that must be presented to any Government functionary on demand. This is an internal passport that everyone must show to authorities for permission to travel within the country, to move to another city, or to apply for a new job.

Having to show "papers" to Government functionaries was bad enough in the era when "papers" meant merely what was on a piece of paper. In the computer era, personal information stored in databases can be used to determine your right to board a plane, drive a car, get a job, enter a hospital emergency room, start school,

open a bank account, buy a gun, or access Government benefits such as Social Security, Medicare, or Medicaid.

While each classification currently has its own set of rules, connecting all these dots would amount to the personal surveillance and monitoring that are the indicia of a police state. The Washington buzz words “information-sharing” are often put forth as the solution to 21st Century problems, but this has significant privacy implications that must be addressed.

Invasions of privacy are no longer limited to Government. Big business has become nearly as powerful in demanding, collecting, sharing, and selling our personal information. Information-gathering and sharing by Big Brother and Big Business raise varying levels of concern, and both are privacy invaders. Government and business often commingle and corroborate their information-sharing in the name of catching deadbeat dads, terrorists, money launderers, drug peddlers, and criminals.

The global economy is obsessed with gathering information. The lifestyle or profile of each consumer is a valuable commercial commodity. The checks you write and receive, the invoices you pay, and the investments you make reveal as much about you as a personal diary. Where I shop, how often I travel, when I visit my doctor, how I save for retirement are all actions known to financial institutions, which connect the dots of my life and create a valuable personal profile. This compilation of personal information is bad enough, but the sharing of it without my consent is even worse.

Thus far, big business has largely been unwilling to exercise self-restraint to respect the privacy of consumers. The bottom-line dollar is viewed as more important. Financial institutions do not want to seek prior express permission to share customer profiles because they know that most people will not sign-up.

True privacy protections encompass the principles of notice, access, correction, consent, preemption, and limiting data collection to the minimum necessary. These form the core of the Fair Information Practices (FIP) first codified in the 1974 Privacy Act, and they should serve as the model for every classification or compilation of personal information.

Three years ago, Congress had the opportunity to dramatically change how financial institutions treat personal information by embracing these core principles, but the resulting law was only a slight improvement over no protections at all.

On November 12, 1999, President Clinton signed into law the Financial Services Modernization bill, known more commonly as Gramm-Leach-Bliley (GLB). This Act included several sections aimed at protecting sensitive personal information obtained and maintained by financial institutions, but in practice, these meager provisions are proving inadequate.

Achieving true financial privacy was conflicted by the underlying goal of GLB, which was to streamline financial services, thereby increasing affiliation and cross-company marketing once affiliated. Greater affiliation meant greater information-sharing. Interjecting the right of individuals to control their personal information into that streamlining equation was perceived as a threat to this big business scheme.

As a result, the GLB sections on privacy were severely watered down. Instead of personal information being kept confidential, financial institutions collect, repackage, and share the data. In some instances personal information is shared with the Government, and in other instances, it is shared with hundreds of other “affiliated” companies. Even under GLB, it is still legal. GLB failed to recognize that consumers are the rightful owners of their personal information. Your financial diary should be your property, not the bank’s.

GLB does not provide consumers with any opportunity to decide for themselves about the transfer of their private information among affiliates. Particularly troubling is the large number of companies marked as affiliates. For instance, Bank of America has nearly 1,500 corporate affiliates, and Citigroup has over 2,700. There is no opportunity to stop this free flow of personal information.

GLB did include a privacy notice provision. Privacy notices should be simple documents outlining what kinds of information are collected and how the business uses that information. However, the notices sent to consumers as a result of GLB turned out to be too complicated for the public to cope with.

When GLB was set to go in effect, few consumers understood their rights. Notices began reaching consumers, and we began receiving questions about them through our website. Making the situation even more confusing, a mass e-mail was sent out by an unknown source claiming that anyone could opt-out of all information-sharing of banking, credit, and other financial records by calling the credit reporting companies. We tried to provide clarification and assistance through a special alert on our website, but financial institutions failed to explain the companies’ privacy policies in simple terms.

GLB also provided the right to opt-out of information-sharing but only to third parties. With all the confusion in the notices, figuring out how to prevent the sale of your personal financial diary, and to whom you were actually denying it, was yet another significant obstacle. Opt-out consent depends on being able to understand what you are saying no to. This is a misplaced burden, especially when combined with complex, unintelligible privacy notices. Again, the design of GLB failed to begin with answering the essential property rights question. The individual was burdened with seeking further explanation of his options and consent rights to ensure protection of his financial diary.

If financial institutions want to offer such a range of popular services, they should have no problem simply explaining those services and letting individuals decide whether they want to sign-up for such offers. The burden should be on the financial institutions to be honest, to better market their products, and to respect the best interests of the customer. This would contribute to more confidence and trust in the customer-business relationship.

One redeeming factor of GLB was in the area of preemption. To the financial institutions' chagrin, GLB set a floor of protections rather than ceiling. Stronger State privacy laws can be placed on top of GLB's limited protections. Some States have already taken action and more are likely to do so. For instance, when the question was put to the people of North Dakota, information-sharing without consent lost by 73 percent. A financial privacy bill in California was narrowly defeated this year, but State legislators are expected to revisit the issue.

The problems with the GLB privacy provisions are clear. Exceptions, such as sharing among affiliates, make notices very complex. Typically buried in small print, the limited opt-out consent burdens individuals, insufficiently protects non-public data, and minimizes the confidence in financial institutions' practices. The banking lobby is working hard to defeat greater financial privacy, but they should embrace better business practices that put their customers' interests first.

It is also important to mention a disturbing trend in Government exchange and reliance on private collections of information, such as through financial institutions. The post-9/11 atmosphere encourages more information-sharing and verification of identity, but any actions should be done cautiously so as to not impact law-abiding citizens.

In 1998, the Clinton Administration proposed a Federal regulation called Know Your Customer, which would have turned your friendly local banker into a snoop reporting to the Federal database called FinCEN any deviation from what the bank decided is your deposits/withdrawal profile. The American people responded with 300,000 angry e-mail criticisms and the regulation was withdrawn. However, the Bank Secrecy Act still requires banks to share personal information with the Government through suspicious activity reports.

The Bush Administration's proposed regulations announced on July 17 to implement the USA PATRIOT Act's Anti-Money Laundering provisions call for identity verification, but they are even more intrusive than Know Your Customer. On that very same day, *The Wall Street Journal* reported that the Treasury Department entered into an agreement with the Social Security Administration (SSA) "to develop and implement a system by which financial institutions may access a database to verify the authenticity of Social Security numbers provided by customers at account opening."

Congress promised us that the SSN would never be used for anything else when it was created, and certainly not for identification purposes. Giving financial institutions access to SSA's database embraces the SSN as a national ID number, which is a step in the wrong direction. Such so-called antimoney laundering provisions are threats to the privacy of law-abiding citizens. Is access to our personal records housed in the Internal Revenue Service the next step?

In conclusion, neither Government nor private business should act as if they can own, share, display, or traffic our personal information without our consent. Our personal financial data should be protected by a firewall and accessible only to those who have authority. Financial institutions are in a unique position of housing our financial diaries that often contain all the dots of life. Extra caution and care should be taken by these corporations to ensure protection not only from fraud but also from misuse and overuse within the companies. Unless financial institutions are willing to raise their privacy standards independently, Congress should revisit GLB to raise the floor of privacy protection for our financial diaries.

PREPARED STATEMENT 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

SEPTEMBER 19, 2002

Chairman Sarbanes and Members of the Committee, thank you for the opportunity to testify before you today. As you know, U.S. PIRG¹ serves as the national lobbying office for State Public Interest Research Groups, which are independent, nonpartisan 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

The Congress knew that the 1999 Gramm-Leach Bliley Financial Services Modernization Act⁴ (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 "nonpublic personal information" subject to strong privacy protection.

STATUS: An important recent decision by the DC Circuit U.S. 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.

¹ U.S. PIRG, www.uspirg.org is the national lobbying office for the State Public Interest Research Groups, www.pirg.org. State PIRG's are nonprofit, nonpartisan 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 nonprofit, nonpartisan, noncommercial publisher of *Consumers Report* 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 www.privacypledge.org.

⁴ Public Law 106-102, 15 U.S.C. § 6801, *et seq.* enacted November 12, 1999.

(2) *Title V required covered firms to provide, by July 2001, annual notice of their information-sharing practices with both affiliated and nonaffiliated 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, nonaffiliated third parties. Transactions between affiliates and also with many nonaffiliated 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)). 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 the GLBA fails to meet the Fair Information Practices (discussed below).

(4) *Title V attempted, through an encryption provision, to restrict the tawdry practice of nonaffiliated 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 do not think they ordered anything, when they do not hand over cash, a check, or a credit card number. Unfortunately, the encryption provision has codified, instead of stopped, the growing epidemic of anticonsumer, controversial "preacquired 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 to 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 should 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 fi-

financial statements and account balances.”⁵ In this case, conservative investors who held maturing certificates of deposits (CD’s) were switched into risky financial derivative products. Some lost large parts of their life savings.

- Second, Minnesota Attorney General Mike Hatch had recently sued U.S. 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 nonaffiliated 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 preacquired account telemarketing. General Hatch has settled with both U.S. 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 U.S. Treasury Department and the Federal Trade Commission seeking stronger laws restricting “preacquired 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 nonpublic 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 nonaffiliated third parties. GLBA then requires firms to grant customers a limited right to opt-out of a small number of transactions with some nonaffiliated third parties (primarily telemarketers).

The opt-out applies to neither affiliates nor any nonaffiliated 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 nonaffiliate 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 caused by unrestricted information-sharing.

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 U.S. 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)).

The inherent weaknesses of the 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 500,000–700,000 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 the 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 "nonpublic personal information" subject to strong privacy protection.

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 June 1999: "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, U.S. 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.

STATUS: An important recent decision by the DC Circuit, U.S. 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 “nonpublic personal information.” The final GLBA financial privacy rules issued by 7 Federal financial agencies defined Social Security Numbers as nonpublic 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 (e.g., for use in a credit report) but not for unregulated purposes, where the credit bureau would be considered a nonaffiliated 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 birth¹⁴ 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 the 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 redisclose 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 pro-

¹⁴In a separate 2001 decision by the DC Circuit, U.S. 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.

vide 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, the 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 nonpublic 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 Commission¹⁷ 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 nonaffiliated 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

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/pretextes.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.

According to a smaller August 2002 California PIRG survey²⁰ of 10 bank privacy notices issued in the second year, 2002: “Most banks received 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 “nonevent” 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 is 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 nonevent 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.

(U.S. 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, nonaffiliated third parties. Transactions between affiliates and also with many nonaffiliated 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 the 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:

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

²¹ See especially paragraphs 21–24 of U.S. 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 FIP’s, “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 FIP’s in the original HEW guidelines, as well as other versions.

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 the 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 the 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.

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) (October 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>.

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). 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 nonaffiliated 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, the 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 do not think they ordered anything, when they do not hand over cash, a check, or a credit card number. Unfortunately, the encryption provision has codified, instead of stopped, the growing epidemic of anticonsumer, controversial “preacquired 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. Preacquired 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 preacquired 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 also 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 the 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. Preacquired account telemarketing should be

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.

banned. We are encouraged that the proposed FTC amendments to the Telemarketing Sales Rule would ban preacquired 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 “preacquired 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 percent–27 percent 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 773²⁸ 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 nonaffiliated 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,

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 percent–27 percent 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.

there will be greater clarity for legislators about States' rights to regulate affiliated transactions.

Recommendations

(1) STRENGTHEN GLBA

Gramm-Leach-Bliley Act should be strengthened. Consumers should be granted an affirmative informed consent right (opt-in) before nonpublic 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 (H.R. 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 Tom 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 insufficient 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.

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/dmfp/privacy.html> or <http://www.cdt.org/publications/dmfp/privacy.pdf>.