AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

H.R. 3997, FINANCIAL DATA PROTECTION ACT OF 2005

HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

NOVEMBER 9, 2005

Printed for the use of the Committee on Financial Services

Serial No. 109–61

U.S. GOVERNMENT PRINTING OFFICE

26–758 PDF WASHINGTON : 2006

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
RICHARD H. BAKER, Louisiana
DEBORAH PRYCE, Ohio
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
JUDY BIGGERT, Illinois
CHRISTOPHER SHAYS, Connecticut
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona
JIM GERLACH, Pennsylvania
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
MICHAEL G. FITZPATRICK, Pennsylvania
GEOFF DAVIS, Kentucky
PATRICK T. MCHENRY, North Carolina

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
CAROLYN MCCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
MELISSA L. BEAN, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
GWEN MOORE, Wisconsin,

BERNARD SANDERS, Vermont

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SPENCER BACHUS, Alabama, *Chairman*

WALTER B. JONES, JR., North Carolina, *Vice Chairman*
RICHARD H. BAKER, Louisiana
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SUE W. KELLY, New York
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
JUDY BIGGERT, Illinois
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
RICK RENZI, Arizona
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
PATRICK T. MCHENRY, North Carolina
MICHAEL G. OXLEY, Ohio

BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
STEVE ISRAEL, New York
CAROLYN MCCARTHY, New York
JOE BACA, California
AL GREEN, Texas
GWEN MOORE, Wisconsin
WM. LACY CLAY, Missouri
JIM MATHESON, Utah
BARNEY FRANK, Massachusetts

CONTENTS

	Page
Hearing held on:	
November 9, 2005	1
Appendix:	
November 9, 2005	41

WITNESSES

WEDNESDAY, NOVEMBER 9, 2005

Bohannon,Mark, General Counsel and Senior Vice President Public Policy, Software and Information Industry Association	23
Brill, Julie, Assistant Attorney General, State of Vermont	25
Callari, Josie, Senior Vice President, Astoria Federal S&L Association and Chairman, America's Community Bankers Electronic Banking and Payment Systems Committee, on behalf of America's Community Bankers	19
Hendricks, Evan, Publisher, Privacy Times	27
Ireland, Oliver I., Partner, Morrison & Foerster LLP, on behalf of Financial Services Coordinating Council	18
Kaufmann, Karl F., Sidley Austin Brown & Wood LLP, on behalf of Chamber of Commerce	28
Lively, H. Randy, President & CEO, American Financial Services Association	21

APPENDIX

Prepared statements:	
Oxley, Hon. Michael G.	42
Ackerman, Hon. Gary L.	44
Baca, Hon. Joe	46
Bachus, Hon. Spencer	47
Biggert, Hon. Judy	50
Clay, Hon. Wm. Lacy	51
Ford, Hon. Harold E., Jr.	52
Gutierrez, Hon. Luis V.	53
Hinojosa, Hon. Ruben	55
Lee, Hon. Barbara	57
Bohannon,Mark	58
Brill, Julie	64
Callari, Josie	81
Hendricks, Evan	86
Ireland, Oliver I.	100
Kaufmann, Karl F.	113
Lively, H. Randy	119

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Bachus, Hon. Spencer:	
ARMA International, prepared statement	122
ID Analytics Corporation, prepared statement	128
Mortgage Bankers Association, prepared statement	139
National Business Coalition on E-Commerce and Privacy, prepared statement	145
Frank, Hon. Barney:	
National Association of Attorneys General, letter, October 27, 2005	152
National Association of Insurance Commissioners, prepared statement	164

Page

Hinojosa, Hon. Ruben:
Texas Business & Commerce Code, Definitions, Section 20.01 168
Identity Theft Enforcement and Protection Act, Texas State Legislature, May, 28, 2005 171

H.R. 3997, FINANCIAL DATA PROTECTION ACT OF 2005

Wednesday, November 9, 2005

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2128, Rayburn House Office Building, Hon. Spencer Bachus [chairman of the subcommittee] Presiding.

Present: Representatives Bachus, Castle, Kelly, LaTourette, Biggert, Tiberi, Hensarling, Pearce, Neugebauer, Price of Georgia, McHenry, Sanders, Maloney, Ackerman, Moore of Kansas, Frank, Hooley, Ford, Hinojosa, Crowley, Baca, Green, Moore, Clay, and Matheson.

Also Present: Representatives Oxley, Pryce of Ohio, and Bean.

Chairman BACHUS. Good morning. There was a Republican conference this morning. And it is just now concluding. So I do expect some Republican members to be arriving in the next few minutes.

Today's hearing is on H.R. 3997, the Financial Data Protection Act of 2005. This is the fourth committee hearing this year on improving data security for consumers.

During the past several years, this committee has passed various pieces of legislation addressing the identity theft issue. Most importantly, the Fair and Accurate Transaction Act, or FACT Act, contained provisions not only preventing identity theft, but giving victims added protections and remedies, particularly restoring an accurate credit report if they were victims of identity theft.

This morning, we will consider data security legislation which will give Americans, American consumers, further protections against credit card fraud, identify theft, and the release of confidential information.

H.R. 3997 was introduced by Mr. LaTourette, Ms. Hooley, Chairman Castle, Chairman Pryce, and Mr. Moore. So it is a bipartisan piece of legislation. It seeks to expand the data safeguard requirements of Gramm-Leach-Bliley Act and the Fair Credit Reporting Act by establishing uniform standards for all businesses that possess or maintain sensitive financial or identity information about consumers.

H.R. 3997 would prevent data breaches by mandating a strong national standard for the protection of sensitive information on consumers, require institutions to notify consumers of data security breaches involving sensitive information that might be used to

commit financial fraud against them, and require institutions to provide consumers with a free 6-months nationwide credit monitoring service upon notification of a breach.

Over the past several months, there have been numerous news reports describing potentially serious breaches of information security. These breaches have generally involved sensitive personal information such as individuals' names, Social Security numbers, or payment card information. Although the reports of subsequent fraud associated with these breaches have been relatively few, protecting customers and consumers after such data breaches obviously remains of primary concern.

Furthermore, data breaches, even if relatively uncommon and limited in scope, undermine consumer confidence. For instance, surveys suggests that the growth of online commerce is restrained due to fears about information security.

Our fundamental goal is to ensure that companies protect sensitive consumer information to avoid potential security breaches. Unfortunately, no data protection program is perfect. Therefore, we need to make sure that companies take reasonable steps to protect consumers in the event that there is a breach.

This morning, we will have a discussion about providing notices to consumers who are affected by data breach in addition to other ways of mitigating consumer harm. These notices should only be sent out when appropriate so as to avoid overnotification of consumers, or customers. In addition, Congress should establish a national uniform standard to protect all Americans from data breaches.

Lastly, data security legislation should distinguish between identity theft and credit card fraud.

H.R. 3997 goes a long way toward achieving these objectives. And I look forward to moving this bill in the near future.

As I mentioned earlier, the sponsors of 3997 should be commended for drafting bipartisan data security legislation.

I also want to recognize the work of Ms. Bean, Mr. Frank, and Mr. Davis on H.R. 3140, the Consumer Data Security and Notification Act of 2005. Like them, I think the time is ripe for Congress to act on data security legislation and our work with the sponsors of 3997 and with the sponsors of 3140, as well as any other members of this committee, on this important legislative initiative.

Let me close by—well, at this point, I will recognize Mr. Sanders, the ranking member, for any opening statement he would like to make and then we will introduce our panel of witnesses, and some of my colleagues wish to introduce certain panelists from their States.

Thank you, Mr. Sanders.

[The prepared statement of Hon. Spencer Bachus can be found on page 47 in the appendix.]

Mr. SANDERS. Thank you very much, Mr. Chairman, and I thank you for holding this important hearing and I am especially pleased that Julie Brill, the assistant attorney general for the State of Vermont, can be with us this morning, and I will be looking forward to her testimony and I will be introducing her in a moment.

Mr. Chairman, identify theft and security breaches at some of our Nation's largest companies are huge issues that this committee

has got to deal with. According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past 5 years, costing businesses, financial institutions, and consumers over $50 billion per year. Victims of identity theft pay an average of about $1,400, not including attorney fees, and spend an average of 600 hours to clear their credit reports.

In addition, Mr. Chairman, over the past year, there have been over 100 security breaches and data leaks at some of the biggest companies in this country, threatening the financial privacy of tens of millions of Americans.

The largest one became public in May of 2005 with Card Systems Solutions, Incorporated, reported a major security breach, potentially compromising over 40 million credit card account numbers. And in February of 2003, the FBI announced a nationwide investigation of a computer database security breach containing roughly 8 million Visa, MasterCard, and American Express credit card numbers. This breach forced many financial institutions to reissue thousands of Visa and MasterCards as a precaution against potential fraud. But we are not just talking about credit card companies. We are talking about Time Warner, Lowes stores, T-Mobile USA, ChoicePoint, Lexis-Nexis, Wells Fargo, Bank of America, and on and on.

For a variety of reasons, Social Security numbers, debit and check credit, check card information, driver's license numbers, e-mails, personal computer files, and information about student loans and mortgages are being stolen by computer hackers and other scam artists.

Mr. Chairman, this has got to stop. We must make sure that hackers and others are protected to the fullest extent of the law, but we must also make sure that the largest and most profitable multi-national companies in this country do everything they can to make sure that identity thieves don't succeed in the first place.

Today we will be discussing one bill that deals with the subject, H.R. 3995, the so-called Financial Data Protection Act of 2005. Mr. Chairman, I have serious concerns about this legislation. As I understand it, this legislation would preempt security breach notification laws in the 21 States that have enacted them to date and would also overturn the consumer credit report freeze provisions enacted by 12 States, including my own State of Vermont. That is wrong.

Mr. Chairman, if Vermont or Alabama want to pass laws that are stronger than the Federal Government's, we should give States that right. That is what Federalism is all about.

The States are laboratories of democracy. If there is a particular identity theft crisis in Colorado and the Colorado State legislature passes a law to correct this problem and it works, what happens? Pretty soon, Maryland may pass the same law, then Nebraska, then Ohio. We learn from each other. And that is one of the very exciting and positive aspects of our system of Government.

But if this legislation is signed into law, we would permanently prevent the States from taking this action.

We hear a lot of talk from our conservative friends about protecting the States and the American people against the big bad and intrusive Federal Government.

And I would hope that today and in this legislation, our conservative friends would honor the mantra that they preach very, very often. Instead of preempting State consumer protection laws, there is another bill that has been introduced by Ms. Bean, H.R. 3140, the Consumer Data Security and Notification Act, that I believe this committee should also seriously consider. As I understand it, this legislation would provide strong consumer protections and enforcements against credit card fraud and identity theft.

H.R. 3140 would strengthen Federal protections against improper collection and sale of sensitive consumer information and provide consumers with advance warning when their personal financial information is at risk.

In addition, the bill contains tough enforcement provisions to protect consumer from identity theft. Most importantly, in my view, this legislation does not preempt States and localities from passing stronger consumer protection laws.

Finally, Mr. Chairman, I strongly believe that this committee should focus on how the outsourcing of financial jobs to China, India, and other cheap foreign labor markets also threatens the privacy of our citizens. According to one study, more than 500,000 financial service jobs in the United States representing 8 percent of all jobs in banking, brokerage, and insurance firms, will move offshore in the next 5 years. This is not just an issue of protecting the working people of this country. It is also an issue of privacy rights.

It seems to me that no financial services firm or credit bureau agency is immune to overseas outsourcing. And this is an issue we have got to focus on.

Mr. Chairman, with growing problems in identity theft and with no domestic legal protection for the privacy of the personal records of American citizens, the situation is unhappily ripe for abuse and the evidence is mounting.

That is why I am supportive of legislation introduced by Congressman Markey that would make it illegal for companies in the U.S. to send financial data abroad without the express written consent of their customers.

Mr. Chairman, thank you again for holding this hearing, and I look forward to working with you on this issue.

Chairman BACHUS. I thank the ranking member. At this time, I recognize the chairman of the full committee, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman. This morning, the committee meets to hear from a number of leading business and consumer groups on H.R. 3997, the Financial Data Protection Act. This bipartisan bill is a product of the hard work and leadership of Representatives LaTourette, Hooley, Castle, Pryce, and Mr. Moore of Kansas. And I congratulate them on their accomplishment. And also I thank the subcommittee Chair, Mr. Bachus, and Ranking Member Sanders for spotlighting this issue in their hearings. This issue will be a priority for the committee when we return early next year. And I look forward to working with the sponsors as well as the chairman and the ranking member.

In recent years, criminals in the United States and abroad have become increasingly inventive in finding ways to access and exploit information systems in order to commit identity theft. According to

the Federal Trade Commission estimate, 10 million Americans are victimized by identity thieves each year, costing consumers and businesses over $55 billion per year. Several recent high profile security breaches have focused public attention as never before on the vulnerabilities of companies' data security systems. This year alone, we have seen nearly 75 breaches impacting over 50 million Americans.

As a result of these numerous breaches, Congress needs to review how information is handled, and what happens when it is mishandled. The Financial Services Committee has worked tirelessly over the past several years to identify and enact solutions to improve data security protections. In 1999, many of the senior members of this committee helped enact the first data security laws in the Gramm-Leach-Bliley Act applying to financial firms.

In 2003, the gentleman from Alabama, Mr. Bachus, led the committee in expanding on this effort by securing the passage of the Fair and Accurate Credit Transactions Act, or FACT Act, which generally expanded consumer idea identity theft protections.

A number of other committees in the House and in the Senate are also working on legislation to address data security protections. This committee must do its due diligence by producing legislation that sets national protection for consumers and supports the financial services marketplace.

We can build on the work we did on the FACT Act to achieve a unified product coming from this committee.

We have a great deal of expertise on this committee on these issues. And I expect that our legislation will be a significant portion of any final House product. We seek to achieve a uniform national standard that protects consumers to a greater overall degree than they are protected now.

H.R. 3997 requires all businesses with sensitive information on consumers to adopt data security, policies and procedures, investigate data security breaches, make uniform notification, and provide mitigation to consumers where there is a likelihood of harm to the consumer.

I applaud the bipartisan cosponsors for putting together a balanced, fair, and reasonable approach for our committee and looking forward to further consideration of this legislation going forward.

Mr. Chairman, again, thank you for your leadership, and I yield back.

[The prepared statement of Hon. Michael G. Oxley can be found on page 42 in the appendix.]

Chairman BACHUS. I thank the chairman and now recognize the ranking member of the full committee, Mr. Frank, who is one of the cosponsors of 3140.

Mr. FRANK. Thank you, Mr. Chairman, and thank you for your opening statement in which you noted that there are a variety of bills because I must say that I am very disappointed with the very version of H.R. 3997 that is now before us. And I would ask you ask unanimous consent at this point to put into the record some explanation of my disappointment. One is a letter from the National Association of Insurance Commissioners, which we just received. Let me read their summary—

Chairman BACHUS. Yes, and without objection, it will be entered into the record.

Mr. FRANK. In short, H.R. 3997 would take away existing State consumer privacy laws, market conduct enforcement authority, and data security safeguards for the purpose of establishing a Federal system that limits consumer protection to being notified under certain circumstances when a breach of data security occurs.

The attorneys general—nearly all of them—I keep trying to count. Sometimes I get 47. Sometimes I get 48. I don't think they have changed. I think my counting changed. But nearly all of the attorneys general have sent a letter, too, to the leaderships basically opposing 3997 in that they talk about a lot of things they want to see in the bill that aren't in 3997. And they have said—and the letters from the attorneys general ought to be included in the record as well. The point they make, and it is a point that I have made and others here have made that governed our activity when we passed the FACT Act dealing with credit. They say on page 2, we call on Congress to enact a national security breach notification law that will provide meaningful information to consumers. If Congress is not able to extract a strong notice law, it should read be issued to State law which is responding strongly.

3997 cuts back on Federal law, interestingly. I was particularly disappointed to see that it would weaken Title V of Gramm-Leach-Bliley. And in many ways, consumers would be worse off than they were before. And what it then does is to undercut, to preempt a lot of State laws. The standard for notification is less. We had a situation with Bank of America, an important institution of my own State in part—I guess in every State. So big deal for me.

But they had a breach. And they had to notify customers because of a California law. Had it not been for the California law, they would not have had to notify anybody. Understand that if this bill passes, 3997, which I do not expect it to, I don't think Bank of America would have had to notify. Now I note some of my friends in the financial service industry have argued that they don't want to too quickly notify people when there has been a breach of the security of the data because of a very new-found concern for the capacity of people's mailboxes.

I have a rule I will tell my friends in the financial services community; try in political debate to avoid saying something that no one will believe. It may seem useful to you in the spur of the moment, but it rarely works. For the financial service industry, which keeps my mailbox quite full with various solicitations for credit cards, mortgages, and all other matter of products, to suddenly decide that the one thing they don't want to send me is a notification that my data has been breached really doesn't persuade anybody.

So we, I think, have to—and the bill that we have filed, and I appreciate your noticing it, Mr. Chairman, when we get to the mark up, I hope it will be obviously considering the subject, not a particular bill, what we try to do is to give an incentive to encrypt the requirement to notify consumers in the bill we have filed, on our side, as most of the Democrats, would decrease the requirement to notify to the extent that the data has been encrypted.

That is, we don't try to put a burden of proof on you to show that—we don't say that it is only to be—there is only to be notifica-

tion if it is pretty clear that there is going to be a breach, but the more you have done things to protect the security of the data, the less likely you are to have to notify.

Similarly, while it is not in our bill, I think a consensus is now developing for a credit freeze. And I will serve notice now that whenever we consider this, there will be an amendment offered to provide for a credit freeze, and I notice, for instance, in the 3997, there is some restriction on liability for the holders of the data.

I would be willing to do that if, in fact, there was a right of a credit freeze and if people would exercise—have the right to have exercise a credit freeze it would limit liability. Otherwise it is too broad. So there are a number of areas where, as I said, I am disappointed in 3997. It weakens Title V, which would seem to me entirely unnecessary to this purpose. It cancels a lot of State laws and puts inadequate Federal laws in their place. So we look forward to the opportunity to work on this.

This committee has been able on most pieces of major legislation to arrive at a pretty good bipartisan consensus. I just want to serve notice today we ain't there yet. And 3997 certainly isn't there. But we hope that we can get there. Thank you, Mr. Chairman.

Chairman BACHUS. Thank you. Let me say this as we move forward and I think, Mr. Frank, and we have had discussions and the chairman and I know the sponsors of the bill, and it is all our intention to work together.

Mr. FRANK. I appreciate that, Mr. Chairman, you have always done that.

Chairman BACHUS. And I think that there is at least some consensus that we will not mark up a bill until January or February.

And one of the reasons for that is we do not have a consensus at this point.

Mr. FRANK. Thank you, Mr. Chairman. Let me say, I think I speak for a very strong bipartisan consensus when I say that this is a very important subject; we hope it is February and not January.

Chairman BACHUS. I think that Chairman Castle and Chairman Pryce and Mr. LaTourette probably agree.

So, thank you. At this time, Chairman Castle?

Mr. CASTLE. Thank you, Mr. Chairman. I also, Mr. Chairman, appreciate the hearing you are holding today on this very important piece of legislation.

We have worked very hard over the past few months, those of us who are involved in this, to develop a comprehensive approach to securing information. In today's hearing, while the fourth in a series on this topic, it is the first that really focuses on this particular legislation. I think each one of us as individuals will agree that we enjoy the convenience that comes with the ability to pay bills online or the ability to apply for a mortgage, car loan, or home equity loan via the Internet. And businesses certainly enjoy greater sales and increased productivity as a result of high speed computer technology that captures vast amounts of consumer information.

But at the same time, we worry about compromising sensitive, personal, and financial information. And we worry about consumers' willingness to share that information especially because in

2005 alone there have been 75 corporate data security breaches involving sensitive information, an estimated 75 million consumers.

The goal of H.R. 3997, the Financial Data Protection Act, is simple, to treat data that is valuable to businesses and consumers with care and to safeguard it from abuse or misuse.

Many States have different standards for the protection of sensitive consumer information and notification in place already. But this patchwork approach to consumer data protection is not ideal. Therefore, I look forward to hearing from our distinguished panelists today about the need for uniform, comprehensive data security requirements to protect sensitive personal information that may be used to commit fraud—especially the crime of identity theft.

I am hopeful that your testimony will shed light on why such a standard is critical for businesses and consumers. Thank you, Mr. Chairman. I yield back.

Chairman BACHUS. Thank you. Ms. Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman. And I welcome all of the participants today as well as all of the witnesses on this important issue. And I would particularly like to welcome Ms. Josie Callari from Astoria Federal Savings, a New York community bank that is located in the district that I am honored to represent.

Our colleagues in Energy and Commerce have started their work, and so it is high time that we do the same. In considering how to address the issue for financial services institutions, we start from a forward position. Since those entities are already subject to the data security and privacy protections in the Gramm-Leach-Bliley Act. Title V of that Act already requires financial service institutions to implement data security safeguards, a customer response program, and a comprehensive privacy policy.

I am sure if you ask the institutions here today that they would be able to describe how they are implementing these programs in detail in their own institutions.

I would say, particularly smaller institutions have paid the price to address data security breaches for their customers, even when the data was lost by a data broker or merchant, because the customer is a bank client and customer relations are important and because they believe in taking care of their clients. And I have heard such stories from the constituents that I represent.

In my view, to the extent that we impose additional national standards, we should be very cautious in how we disrupt the newly settled system of regulations that has been put in place under Gramm-Leach-Bliley. On the other hand, we need to make sure that our financial institutions aren't paying the price for other less well regulated. It makes no sense to have a national system that provides different consumer protections to the same sensitive financial information depending on who lost it.

For example, data brokers who lose information should bear the burden of compensating for those losses and protecting consumers in the future.

There are several issues, however, that the implementation of Gramm-Leach-Bliley has shown up as a weakness in the data protection according to our financial institutions. And one of those issues that my constituents are extremely concerned about—and I am sure that this is probably true across the Nation—is what pro-

tections do consumers have when their data is sent overseas to be processed?

Many countries don't have data security protections that are as robust as those that we have in this Nation. Yet financial services companies routinely use data processing services to process sensitive financial information.

So I will definitely be offering the Markey bill and the proposal that strengthens the oversight of data that is sent overseas. And I feel that should be strongly addressed in this legislation.

I would also like and request the chairman to place in the record a letter that has come to me and probably many others from the attorneys General across this Nation. And they argue that States should have the ability to enforce any national security breach notification laws and that State laws should be left to govern entities not covered by the Federal law or the consequences of security breaches. Their letter was signed by many attorneys general, including New York's Attorney General, Eliot Spitzer.

On the other hand, some of my industry representatives have argued that only if State laws are completely preempted will financial institutions be able to cope with the compliance issues that data security presents and that functional regulators are best equipped to enforce regulations governing the entities with which they are familiar.

So in your comments, I wish that the panelists would address the letter from the attorneys general and your interpretation and advice on it. I thank the chairman. I have been—I have learned over many years that many contentious issues I think will never ever be in agreement. But often you have bent over backwards to listen to the democratic side and we have come forward with a bipartisan agreement on what is fundamentally important to all Americans and that is a strong safety and soundness in our financial system, and I feel confident we will be able to do that and I thank you for your accommodation in the past and look forward to working with you on this bill.

Chairman BACHUS. Thank you. And one thing that Chairman Oxley wanted me to stress and Ranking Member Frank, and I know they have talked, and I believe I speak for both of them when they say that addressing this issue is a top priority of the committee.

And as Mr. Frank said, if he thinks that February is more appropriate for beginning to mark up a bill, then February it will be, because we need some consensus and agreement going forward.

At this time, I recognize Mr. LaTourette, who is a lead sponsor of the bill.

Mr. LATOURETTE. Thank you very much, Chairman Bachus, and I would ask unanimous consent to include a rather lengthy statement into the record. I want to thank the cosponsors of this legislation, Mike Castle and Debbie Pryce and Dennis Moore and Darlene Hooley. And I was sitting next to Mr. Hensarling when the distinguished ranking member of the committee, Mr. Frank, was talking. And he said to Darlene and to Debbie and to Mike and to Dennis it is like he called our child ugly. And that is too bad. But we worked hard on this legislation.

We recognize that there are competing opinions. But clearly, this is an important issue. The great thing about this committee is it does work together well on most issues in a bipartisan fashion. And as I read the testimony of those who are testifying today, I know that some of you are going to be critical of the bill and some of you are going to be very critical of the bill.

And I just want you to know that if we are going to get this right, we do need the input of everybody. And so we appreciate your being here to offer your observations because I think the one thing that we would like to see at the end of the day is a piece of legislation that, in fact, addresses this rather serious problem.

And while we often debate the issue of preemption and whether or not the 50 States are great laboratories of democracy, and I agree and with the system of Federalism, but I would also suggest that there are times when we need to look at the great ideas that are going on in some of the 50 States and apply them, in some instances, in a limited basis to a national problem.

Mr. SANDERS. Would my friend yield on that?

Mr. LATOURETTE. I would be happy to yield.

Mr. SANDERS. I agree with him. The point is we should take the best ideas at the State level and apply them at the Federal level. But we shouldn't preempt the States from continuing to go forward. That is the main point that I would make.

Mr. LATOURETTE. The appreciate the gentleman's observation, and I know that he holds that clearly and on some issues I agree with him and some I don't agree with him. And we can move that forward as we debate this legislation. But I think that the prime—with all of its warts and flaws, H.R. 3997 is, in fact, a collaborative effort. It is a bipartisan effort. It was an attempt to be thoughtful. And I'm proud of the product and I am very thankful to my co sponsors and Mr. Chairman—

Mr. FRANK. Would the gentleman yield?

Mr. LATOURETTE. I would be happy to yield.

Chairman BACHUS. We probably need to restrict this to opening statements. I will let the ranking member—

Mr. FRANK. Just briefly. The gentleman said that I called a child ugly. And I would just plead guilty and say that it seems to me the obligation to declare all children beautiful should not be construed as extending beyond the boundaries of your own district.

Chairman BACHUS. We are obviously building a consensus already. We are off to a good start.

Mr. LATOURETTE. And I thank the gentleman very much and perhaps we will put braces on the child as we move forward in this process. But I look forward to a rather spirited debate. And Mr. Chairman, I thank you for your leadership and—your committed leadership in not only this issue, but identity theft, not only as we move forward, but in the past. And I yield back my time.

Chairman BACHUS. Mr. Ackerman.

Mr. ACKERMAN. Thank you, Mr. Chairman, and thank Mr. Sanders as well for introducing this legislation at today's hearing. I think it is as good as any of a stepping off point. I do have some very grave concerns about the bill as it has been thus presented. Many of which have been expressed here. I am concerned that in

our rush to do something that must indeed be addressed as expeditiously as we can, that we do get it right.

And citing those things in my opening statement, that have already been expressed, as well as some others with the Chair's assurance that he has given, and true to form that he has always worked and listened to all members of the committee—some of whom might be uglier than others, I am not sure and I don't want to get into that—I would ask unanimous consent to put the entire statement in.

And with the Chair's permission, as I have a markup down the hall at this time, I would like to just say a word of introduction to a constituent who is on today's panel and—

Chairman BACHUS. Yes, that would be fine.

Mr. ACKERMAN. Thank you, Mr. Chairman, very much. I would like to give a special welcome to Josie Callari of Astoria Federal Savings, who is also mentioned by Ms. Maloney, who said that she had their banks in her district, and indeed she does.

It should be noted that there are 18 Members of Congress who represent parts of our city, New York City, or Long Island, and indeed I think if you asked almost any of us, we do have branches of that bank in our district. But I am proud to say that their headquarters in Lake Success is indeed in my district.

Mr. Callari has 30 years of experience in the banking industry and is currently a senior vice-president and the director of banking operations at Astoria Federal savings. She also serves as the vice chairman of the America's Community Bankers Electronic Banking and Payments Committee. And she is ideally suited to provide testimony before the subcommittee today.

And finally, she has been very active as a volunteer and as a supporter of so many community organizations in my district and throughout our region that I would like to thank her personally for that volunteer service as well.

And thank you for coming down. And thank you for participating in this panel. And don't be nervous.

[The prepared statement of Hon. Gary L. Ackerman can be found on page 44 in the appendix.]

Chairman BACHUS. Thank you.

Several opening statements have referenced the attorney general's letter and the attorney general or assistant attorney general; Ms. Brill from Vermont, has actually attached that to her testimony. So it will come in as part of that testimony.

At this time, I recognize Ms. Pryce.

Ms. PRYCE OF OHIO. There is two. I will just submit my statement for the record.

Chairman BACHUS. Mr. Hensarling.

Mr. HENSARLING. Thank you, Mr. Chairman, and I certainly thank you for holding this important hearing. I want to thank my colleagues on this committee, particularly Mr. LaTourette, who collaborated to introduce H.R. 3997.

As we all know, this year there have been numerous widely reported breaches of security in several companies involved in the collection and dissemination of consumer data. This is clearly troublesome.

There is no doubt that companies should have data security policies and procedures in place to protect against fraudulent activity, especially identity theft, the fastest growing white collar crime in America.

In fact, the Federal Trade Commission has estimated that about 10 million Americans fall victim to identity theft every year. I have been one of them. It costs consumers and businesses more than $55 billion in the aggregate.

But, Mr. Chairman, many regulations are already in place that work to protect the personal information of individuals. And we all know that financial institutions in particular are highly regulated under Gramm-Leach-Bliley when it comes to the collection of consumer data. We also know that the Fair Credit Reporting Act, as amended by the FACT Act, helps consumers improve the accuracy of information about them while restricting the disclosure of that same information.

While regulation clearly helps to direct financial institutions' response to identity theft, the actions taken by financial institutions on their own should not be dismissed.

The overwhelming majority of institutions already offer their customers information on how to prevent identity theft and what to do about it, and they train their employees to protect the security of customer information and to assist victims. It is in their interest to do so.

Who wants to tell prospective customers, please allow me to handle your sensitive consumer data; we only had 14 data security breaches last month. Markets can work. They can punish bad or negligent behavior. Just ask anyone who used to work for Arthur Andersen. Ask an investor in ChoicePoint who saw their stock fall almost 10 percent. As Chairman Greenspan told this committee back in July, ″the self interest of people who handle data is so extraordinarily high, I just balk at the notion that anyone has to tell them what their self interest is. I cannot believe that we need regulations to tell people how to make a profit.″

I do think we need to make sure as a body that we are always cautious not to create a remedy that proves worse than the disease. And, unfortunately, Congress has on occasion excelled at the art of unintended consequences.

So I hope, Mr. Chairman, as we consider this important data security legislation, that we keep Chairman Greenspan's words in mind. We know that data security is a serious subject. We also need to ensure we take no action that would needlessly stifle competition or impose unreasonable costs on participants that ultimately will be borne by the consumers. Thank you, and I yield back.

Chairman BACHUS. Thank you, Mr. Hensarling. At this time I recognize one of the cosponsors of the 3997, Mr. Moore.

Mr. MOORE. Thank you, Mr. Chairman. I would like to thank you for holding today's hearings, and I introduced this legislation with Mr. LaTourette, Deborah Pryce, Mike Castle, and Jeb Hensarling, and I want to thank each of my cosponsors. We have all seen this year that breaches of data security are serious and ongoing problem in our country.

The testimony of Vermont's assistant attorney general, Julie Brill, notes that there have been reports of over 118 data leaks this year, which all together have affected 57 million consumers in the United States.

Today 23 States have enacted breach notification laws. Just 2 weeks ago, 47 State attorneys general sent a letter to Congress on the issue of breach notification legislation. I don't agree with all of the statement's recommendations in the letter, but I do appreciate the fact that the attorney general's recommendations that Congress enact a national security breach notification law that will provide meaningful information to consumers.

Unfortunately the State of Kansas has not considered or enacted consumer notification legislation. And our attorney general did not sign the attorneys general's letter. A Federal law that sets a uniform national standard will benefit I believe both consumers and businesses that operate in the State of Kansas.

Further, the passage of notification laws by nearly half the States is a strong indication that there is a problem which does not recognize State lines, and it is in need of a national solution. I believe that solution is embodied in H.R. 3997.

H.R. 3997 would, for the first time, in Federal law, create a uniform consumer notification standard and require companies to notify consumers when their sensitive personal information has been accessed in a way that could lead to substantial harm.

It seeks, I believe, to strike a reasonable balance that requires breached entities to notify but not over-notify consumers when sensitive personal information has been compromised. Believe it or not, I know some of you won't believe this, but sometimes Congress overreacts to certain problems that are presented to Congress. As Congress considers data security legislation, we need to react to a very real problem without overreacting. And I hope that this is contained within 3997.

The bill sponsors, and I believe there should be a few guiding principles behind any data security legislation or bill that is passed by Congress. Number one, companies should be required to safeguard their data. Number two, breached businesses should be required to notify consumers, law enforcement regulators, and relevant third parties when sensitive personal data is compromised, Number three, breached entities need to ensure that consumers are protected after their data is compromised, Number four Federal preemption is necessary, I believe, to create a meaningful uniform national standard. Our legislation embodies each of these guiding principles.

I am proud of this committee's bipartisan work in drafting H.R. 3997. Protecting data and consumers is not a partisan issue, should not be a partisan issue, and the process of drafting and passing data security legislation should and will be bipartisan. Thank you, Mr. Chairman.

Chairman BACHUS. Thank you, Mr. Moore. And I appreciate your work and Ms. Hooley's work on the legislation.

At this time, I recognize Ms. Kelly for her opening statement, and I will also commend your work on oversight committee in this regard.

Mrs. KELLY. Thank you, Chairman Bachus. I appreciate your holding this important hearing.

America demands that its data be secure. The horror stories of recent data leaks weaken the confidence in the security of transaction data and electronic payment systems.

Small businesses, in particular, suffer when they lose access to credit card systems and they are forced to invest in ever more complex and expensive security because of failures at some of the largest companies in the Nation.

The Oversight and Investigations Subcommittee that I chair looked into several of these cases and found that while all involved sought to do the best of their ability to protect consumer data, very few considered the impact on our nationwide economy and small businesses when their best efforts weren't good enough.

I am pleased that the legislation before us protects small businesses while providing clear standards on data protection and loss notification all companies can use.

National standards combined with small businesses flexibility are the hallmarks of this legislation, and they should be a portion of any data security legislation that is considered by the House of Representatives in this Congress.

I am very interested in hearing the comments of our panel today. I thank you and yield back the balance of my time.

Chairman BACHUS. I thank you. Ms. Hooley, at this time, you are recognized for an opening statement as one of the cosponsors.

Ms. HOOLEY. Thank you, Chairman Bachus and Ranking Member Sanders, for holding this subcommittee hearing on H.R. 3997, the Financial Data Protection Act of 2005. I would also like to thank Chairman Oxley and Mr. Frank for their leadership on this issue.

It is imperative that Congress act to make certain that sensitive personal information is protected by adequate safeguards. And I look forward to working with my colleagues on the committee to move this process forward.

Identity theft represents a fundamental threat to e-commerce, to our overall economy, and our homeland security.

No longer are we facing just hobbiest hackers looking to create a nuisance. Increasingly, these attacks are driven by skilled criminals. ID theft is big business.

Since drafting my first identity theft bill with Representative LaTourette in 2000, the number of incidents reported to FTC has increased by eight-fold

Congress made progress from protecting consumers from ID theft in the 108th Congress with the passage of the FACT Act, which provided landmark consumer protections, including free annual access to credit reports from all three major credit bureaus so that consumers could closely monitor their own credit.

I believe this is a great opportunity for this committee to build on that success.

While our free credit report law has helped consumers spot fraud, this new legislation will help stop fraud. For nearly a year now, the sponsors of this legislation, Mr. LaTourette, Mr. Castle, Ms. Pryce, Mr. Moore, have worked with other members of this committee, industry leaders, consumer groups, and victims to write

legislation that safeguards sensitive consumer information, fight ID theft, and create uniform standards for notifying consumers.

What this bill does is very simple. If a business has a sensitive financial information of a consumer, they have a duty to protect that information. Businesses have a duty to investigate, even if they only think there might have been a breach. If that breach might have occurred, they have to notify Secret Service; they notify their regulator if that data is lost or stolen and the consumer is placed at any risk of either account fraud or ID theft, the businesses have to notify the consumer.

This bill requires that there is a single standard easy-to-recognize notice so that consumers won't treat this as junk mail. This bill also requires that notices contain meaningful, useful information to help consumers respond and protect themselves, including the toll free number. And finally, if a consumer is at risk of ID theft, this bill requires that businesses provide those consumers with 6 months of free credit monitoring service so the consumers know that they are victim of ID theft.

This bill will help stop fraud. And I look forward to working with my colleagues to move the process forward. And I thank you and I yield back. Thank you, Mr. Chair.

Chairman BACHUS. Any other members on the Republican side that have opening statements?

Any members? Mr. Green? Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman, for holding today's hearing on proposed legislation intended to stem the increasing number of identity theft cases and data security breaches that are threatening our Nation's economy.

I am hopeful that our efforts to develop a meaningful and measured response will provide assurance to all consumers that their information will be protected from those with impure motives and criminal intent.

The cost associated with identity theft and security breaches are staggering when accounting for both economic and personal damages. In addition to approximately $55 billion in annual losses among both individuals and industry, consumers are often subject to legal and financial obstacles while attempting to reestablish their credit worthiness.

As we develop an appropriate legislative response to these threats, I hope we can build off the model of strengthening data security requirements contained in Gramm-Leach-Bliley for industry members that remain unregulated.

Furthermore, I believe that a uniform Federal standard for security will ensure that both industry and consumers are operating within one set of standards without ambiguity and variances from State to State.

If we want to preserve the optimal benefits of our growing e-commerce sector, then we must create an environment that protects the personal information of consumers in all circumstances while weeding out predatory industry participants.

Thank you, Mr. Chairman. And I yield back the balance of my time.

[The prepared statement of Hon. Wm. Lacy Clay can be found on page 51 in the appendix.]

Chairman BACHUS. Thank you. Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman, and I thank the ranking member as well for hosting these hearings. Mr. Chairman, I am hopeful today that we will get some questions answered that are of concern. Our questions, such as who should determine whether the harm element is met, should it be the consumer reporter as defined in H.R. 3997? Or should it be the breached entity in concert with law enforcement, as the attorneys general recommend? Should this harm element be a trigger to give consumer notice of breach or should consumers always be given notice unless there is no risk of harm resulting from the breach?

And finally, if the breached notification system is overly broad, do we run the risk of inundating consumers with notices and having them ignore important information they may need to protect themselves? I yield back the balance of my time.

Chairman BACHUS. And I apologize. I had a list of members that I thought wanted to make opening statements. Mr. Crowley, Mr. Baca, so.

Mr. CROWLEY. I thank the chairman. I am going to be very brief. I just want to thank the Chairman and the ranking member, Mr. Sanders, for holding this hearing and I look forward to the testimony of all the expert witnesses that are before us today. I want to thank my colleagues on both sides who are conducting I think once again the spirit of this committee, a bipartisan effort to bring about legislation out of this committee. Once again, I hope when legislation that is passed in this committee in a bipartisan effort makes its way to the floor that it is not too diminished by outsiders that make it more difficult for members of this committee to support something on the floor of the House once it gets there from this committee.

But I, too, am looking for a uniform Federal standard, Federal preemption, one that protects the consumer as well as the institutions, one that moves towards—institutions towards encryption and the use of modern technology to help secure the data of consumers in this Nation, one that will maintain or strengthen consumer confidence, a defined trigger and assignment of responsibility where it truly belongs.

And again, I thank all my colleagues, especially Ms. Hooley, who has been very, very engaged in this because of personal experience in her own life. So I do appreciate her involvement and all my colleagues for working in a bipartisan spirit. And with that I yield back.

Chairman BACHUS. Mr. Baca.

Mr. BACA. Thank you very much, Mr. Chairman. I have a prepared statement I would like to enter for the record and suspend with reading it other than just stating that I am very much concerned that H.R. 3997 preempts the State law and ignores the lessons we have learned from the State of California and, of course, like everyone else, has indicated we need a national standard that protects personal information and ensures the consumers receive notices when their personal information is breached. And with that, then, I will submit my statement for the record.

[The prepared statement of Hon. Joe Baca can be found on page 46 in the appendix.]

Chairman BACHUS. Thank you. Are there any other members of the minority? Ms. Bean.

Ms. BEAN. Thank you, Mr. Chairman. I appreciate the opportunity to speak. I would like to thank Chairman Bachus and Mr. Sanders for holding today's important hearing to consider how to best improve data security for consumers.

There is no doubt that as the volume of personal information held by corporations, data brokers, and businesses continues to increase, the issue of data security and protecting Americans' personal information takes on particular importance.

While I am interested, like my colleagues, to hear the testimony and insights from this distinguished panel today and to how Government and industry can work together to better ensure that our consumers' personal information is adequately protected, I would like to take this opportunity to highlight the fact that in addition to H.R. 3997, other pieces of legislation addressing data security have been introduced in the 109th Congress and are pending before this subcommittee. In particular, in June, I joined with Mr. Davis and Mr. Frank in introducing H.R. 3140, the Consumer Data Security and Notification Act of 2005. I believe by considering multiple proposals and approaches, we will ultimately arrive at stronger final product to improve data security.

For example, on controversial issues such as the notification trigger, I look forward to working with my colleagues to accomplish that task. Thank you, Mr. Chairman. And I yield back the balance of my time.

Chairman BACHUS. Thank you. Mr. Matheson, did you—oh, okay. You don't have an opening statement.

If there are no more opening statements, I will say this, Ms. Bean. In my opening statement I did recognize that you and Mr. Frank and Mr. Davis have introduced H.R. 3140, and it is the committee's intent to work with you and with all members to construct a comprehensive approach. So we will be doing that. And you have my assurances that we will work with you.

At this time, I would like to introduce all the panelists. Ms. Callari has already been introduced. I will skip over her and when we get on the attorney general—assistant attorney general, Mr. Sanders will introduce her.

We have with us today Mr. Oliver Ireland, partner of Morrison and Foerster, on behalf of the Financial Services Coordinating Council. Mr. Randy Lively, president and CEO of the American Financial Services Association, welcome you back before the committee; Mr. Mark Bohannon, general counsel and senior vice president of policy of the Software and Information Association; Evan Hendricks, publisher of Privacy Times; and Karl Kaufmann, Sidley—is that Sidley.

Mr. KAUFMANN. Yes, sir.

Chairman BACHUS. Sidley Austin Brown & Wood, LLP on behalf of the Chamber of Commerce.

Mr. Sanders.

Mr. SANDERS. Thank you very much Mr. Chairman.

I am delighted to welcome Julie Brill to be a panelist with us today. She has been an assistant attorney general for the State of Vermont since 1988. She is co-chair of the National Association of

Attorneys General Privacy Working Group. Ms. Grill has spearheaded Vermont's legislative efforts in a wide variety of areas affecting consumers, including privacy, fair credit recording, tobacco, and antitrust. In 2001, she received the Brandeis Award from Privacy International for her work in Vermont and nationally promoting consumers interests in privacy issues. We are glad that she is with us today.

Chairman BACHUS. Thank you. We look forward to hearing from all of witnesses, and I thank them for taking time from their busy schedules. We do anticipate votes on the House floor sometime between 12:15 and 12:45, so if you are wondering about a break, that is apparently the first time we will break unless there is a need to prior to that. If you would just advise us of that, we will be glad to take a short break or excuse you for a minute from the hearing.

At this time, I recognize Mr. Oliver Ireland, and as Mr. Ireland begins his testimony, I am going to have to be excused for a vote in Judiciary. Mr. Hensarling is going to take my place in the Chair. But I have read the testimony.

STATEMENT OF OLIVER I. IRELAND, MORRISON & FOERSTER LLP, ON BEHALF OF FINANCIAL SERVICES COORDINATING COUNCIL

Mr. IRELAND. Thank you, Chairman Bachus, and members of the committee. My name is Oliver Ireland, a partner in the D.C. Office of Morrison & Forester, and I am here today on behalf of the Financial Services Coordinating Council, which consists of the American Bankers Association, the American Council of Life Insurers, the American Insurance Association, and the Securities Industry Association. Together these associations represent a broad spectrum of financial services providers, including banks, insurance companies, and securities firms. Our members have a strong interest in protecting our customers from identity theft and account fraud. Identity theft occurs when a criminal uses information relating to another person to open a new account in that person's name. In addition, in some cases, information relating to a customer's account can be used to initiate unauthorized charges to those accounts. The issues of identity theft and account fraud and related concerns about data security are of paramount importance to financial institutions and the customers that they serve.

In my testimony, I would like to emphasize three key points. Financial institutions have a vested interest in protecting customer information and are highly regulated in this area already. A uniform national approach to information security is critical, and security breach notification requirements should be risk-based.

Financial institutions have long recognized the importance of protecting customer information. Financial institutions incur significant costs from identity theft and account fraud. Accordingly, financial institutions aggressively protect sensitive information relating to consumers. Among those that handle and process consumer information, financial institutions are among the most highly regulated. The Federal banking agencies and the Securities and Exchange Commission have established regulations or guidance covering the security of customer information under Title V of the Gramm-Leach-Bliley Act. In addition, 34 States have established

standards for insurance companies with respect to safeguarding customer information.

We believe that a uniform national approach to security and security breach notification that applies to all financial institutions and non-financial institutions alike but recognizes existing Federal Gramm-Leach-Bliley requirements is critical to preserving efficient national markets and providing consistent protection for consumers. A number of State legislatures have passed security breach notification laws. While these State laws have similarities, they also have important differences. State laws that are inconsistent result in both higher costs and uneven consumer protection and, in some cases, could lead to delays in providing notices. Moreover, an individual State requirement or an individual State's failure to recognize a key provision can effectively nullify the policy choices of other States.

Finally, notification requirements should be risk-based. While it is important to protect all sensitive customer information from unauthorized use, it is most critical to protect consumers from identity theft and account fraud. Security breach notification requirements should be limited to those cases where the consumer needs to act to avoid substantial harm.

Security breach notification requirements should provide clear triggers for notice and should be tailored to the circumstances and to the threat presented. We are pleased that H.R. 3997 is consistent with these goals. H.R. 3997 seeks to establish uniform national standards that apply broadly to virtually all entities that maintain sensitive information. At the same time, it recognizes that financial institutions must comply with existing Gramm-Leach-Bliley Act requirements and attempts to ensure that these requirements are consistent across the financial holding company structure. Finally, H.R. 3997 provides an effective risk-based notification scheme that does not require unnecessary notices to consumers. While we believe that some issues raised by H.R. 3997 still require further resolution, we will be happy to work with the subcommittee to resolve these issues so that this important legislation can move forward. Thank you. I will be happy to answer any questions that you may have.

[The prepared statement of Oliver I. Ireland can be found on page 100 in the appendix.]

Mr. HENSARLING. [presiding.] Thank you for your testimony, Mr. Ireland, and thank you for staying within 5 minutes.

Ms. Callari, you are now recognized.

STATEMENT OF JOSIE CALLARI, SENIOR VICE PRESIDENT, ASTORIA FEDERAL S&L ASSOCIATION AND CHAIRMAN, AMERICA'S COMMUNITY BANKERS ELECTRONIC BANKING AND PAYMENT SYSTEMS COMMITTEE, ON BEHALF OF AMERICA'S COMMUNITY BANKERS

Ms. CALLARI. Thank you.

Thank you, Mr. Chairman, Ranking Member Sanders, and members of the committee.

My name is Josie Callari, senior vice president of Astoria Federal Savings in Lake Success, New York. I am here today testifying on behalf of America's Community Bankers, where I serve as chair-

man of the ACB Committee on Electronic Banking and Payment Systems. ACB appreciates having the opportunity to testify before the subcommittee on H.R. 3997, the Financial Data Protection Act.

The issue of data security is critical for community banks. While banks have had the mandate to safeguard sensitive customer information for years, the growth of the internet and electronic commerce has made compiling and selling sensitive information easier for a multitude of companies. That is why ACB supports H.R. 3997, which we believe focuses on stopping the misuse of consumer information and creates an incentive for companies to make securing customer data a priority.

Earlier this year, ACB board of directors laid out its top priorities for any data security legislation that may be considered in Congress. ACB is pleased to see that this bill addresses several of our top priorities and begins to deal with the difficult issues of reimbursement.

Having a national standard is critical for any legislation addressing data of security and consumer notices. Adding another layer of regulation to a rapidly growing patchwork of State and local laws hurts consumers, hurts the economy, and will not provide effective protection. A patchwork of State laws that provide protection that stop and start at State lines will not provide meaningful full protection for consumers in a national marketplace. Additionally, ACB believes that Congress should recognize that the GLBA already requires financial services companies to have in place much of what is being considered in most data security legislation. Title V of GLBA requires financial services companies to implement data security safeguards, a customer response program, and a comprehensive privacy policy.

This spring, banking regulators issued guidance extending Title V to require customer notices in case of a breach that puts consumers at risk. To layer a duplicative regulatory system on top of this robust framework would only increase costs for financial institutions and ultimately their customers. Likewise, financial institutions have an incredibly robust regulatory framework under which they operate. This is particularly true for depository institutions. ACB applauds the legislation for embracing this existing framework by vesting enforcement with functional regulators.

Finally, ACB supports efforts to ensure that banks have the ability to be part of an investigation into possible breaches. Furthermore, requiring that contracts between companies and third parties specify who is responsible for sending notices is very important. Community banks are proud of the relationship they have with their customers and generally would prefer to be responsible for sending those notices.

Mr. Chairman, there are two areas where ACB members have concerns, and we look forward to working with the committee and the bill sponsors to address them. First and foremost, ACB believes that those who are responsible for data breaches must be responsible for the costs of protecting consumers from risks arising from those breaches. One of the biggest costs associated with the breach is that of reissuing credit and debit cards and closing accounts that are placed at risk. These costs can mount quickly, and community banks end up bearing all of them. Community banks are doing this

now because they are dedicated to protecting their customers. However, those responsible for breaches should bear these costs.

Finally, ACB's members have expressed concern that there is no limit on how long investigations required under the bill can take. ACB members are concerned that without guidance the investigation could take an excessively long time, leaving consumers at risk. We believe the bill should require that regulators give guidance on the appropriate length of an investigation.

In conclusion, ACB supports H.R. 3997 and urges the committee to consider it soon. ACB urges that the bill be passed with constructive modifications such as those suggested but without adding provisions that take the bill's focus away from stopping the misuse of consumer information. We look forward to working with you as the committee crafts legislation that best addresses the problems of data security breaches. Thank you.

[The prepared statement of Josie Callari can be found on page 81 in the appendix.]

Mr. HENSARLING. Thank you, Ms. Callari.

Mr. Lively, you are now recognized for 5 minutes.

STATEMENT OF H. RANDY LIVELY, PRESIDENT & CEO, AMERICAN FINANCIAL SERVICES ASSOCIATION

Mr. LIVELY. Thank you, Mr. Chairman, ranking members.

Mr. HENSARLING. You need to press the button there, please.

Mr. LIVELY. Ranking member and members of the subcommittee. I am Randy Lively, the president and CEO of the American Financial Services Association here in Washington, D.C. It is my honor and pleasure to be here this morning to testify in support of H.R. 3997, the Financial Data Protection Act of 2005, introduced by Representatives LaTourette, Hooley, Price, Castle, and Moore and cosponsored by a broad bipartisan array of this distinguished committee.

The American Financial Services Association represents the Nation's market rate lenders providing access to credit for millions of Americans. AFSA's 300 member companies include commercial and financial companies, auto finance companies, credit card issuers, mortgage lenders, and other financial services firms that lend to consumers and small businesses.

I am proud to say that, next year, AFSA will celebrate its 90th birthday as the Nation's premier consumer and commercial credit association. As I mentioned at the outset, I am pleased to be here this morning to speak in support of the Financial Data Protection Act and ask you, Mr. Chairman, to have the committee give it expedited consideration. AFSA and its members believe that well informed, proactive consumers are our best defense and our first line of attack in protecting all of us from the dangers of identity theft.

According to the Federal Trade Commission, as we have heard earlier today, identity theft robs the Nation of more than $50 billion annually. Consumer losses account for about $5 billion of the total, and business absorbs the remaining $45 billion. Yet, in addition to the immediate monetary loss suffered, AFSA companies are more concerned about losing the trust of treasured customers, and mishandling of a security breach can cost us customers. Obviously,

the best way to protect our customers' information is to prevent a security breach from occurring in the first instance.

Toward that end, AFSA member companies are focusing on training our own employees in the handling of sensitive personal information and are scrutinizing the practices of third party vendors who store or dispose of data which may contain personal financial information. There is no doubt that the industry needs to regularly upgrade and improve the practices and procedures of our own companies and our storage and disposal vendors to prevent security breaches from ever occurring in the first place.

AFSA member companies share this committee's goal of wanting to assure American consumers that their personal information is safely protected. To accomplish this goal, AFSA members are regularly improving their security measures and procedures to prevent thefts to their information systems. H.R. 3997 provides a clear and concise framework for AFSA member companies and other financial services providers to follow in the event of a data breach.

The authors of the Financial Data Protection Act of 2005 clearly understand that an effective breach notification and reaction system must be based on a substantial risk to the customer as well as the businesses that rely on the integrity of the data. If the breach notification system is overly broad, we run the risk of inundating our customers with notices and having them ignore important information they may need to protect themselves. H.R. 3997 establishes a reasonable and balanced approach for businesses and regulators to protect potential breaches of data security as well as uniform procedures to follow if one does occur.

The legislation appropriately anticipates that some breaches may pose a significant risk or harm or inconvenience to consumers whereas other breaches may not create a significant risk for the consumer. This distinction will enable businesses to maximize their vigilance over consumer data, apply law enforcement and regulatory resources where they are most needed, and focus consumers attention to take steps to protect themselves when they are truly at risk.

The Financial Data Protection Act of 2005 calls for—calls on business to conduct an immediate investigation to assess the nature and scope of the breach when it learns that a breach has occurred. The investigation will determine whether the breach has created a substantial risk for the customers personal financial information. The determination will take into account what information has been exposed and whether the information was encrypted, redacted or requires technology that is not commercially available. AFSA believes that the committee should direct the functional regulators to treat the breach of encrypted information as not creating a potential substantial harm unless an actual harm can be demonstrated. In other words, there should be a presumption that the acquisition of encrypted information does not create a substantial risk for consumers to whom information relates. Should a business determine that a substantial breach has occurred, H.R. 3997 directs a company to notify the Secret Service and the appropriate functional regulators as well as third parties that might be affected by the breach. This type of coordinated framework will ensure that ongoing law enforcement investigations are not compromised by

premature publication of breaches. At the same time, the legislation provides reasonable parameters so that a delay in notifying consumers does not unnecessarily extend their exposure to risk of harm. H.R. 3997 directs that breach notices to consumers must be done in a clear and conspicuous manner that describes the nature of the breach, when the breach occurred, the relationship between the consumer and the entity who suffered the breach, and actions that the business is taking to restore the security and confidentiality of the breached information.

AFSA wholeheartedly agrees with the sponsors of H.R. 3997 and directing Federal regulators to work together to create uniform security standards and policies for each business to implement and to maintain to protect sensitive information. Moreover, a uniform national standard replacing the patchwork of varied and numerous State and local requirements will avoid needless duplication that could lead to confusion and divert resources from the actual problem.

Finally, I want to compliment the authors of H.R. 3997 for their foresight in determining that a company is in compliance with data security policies anticipated under this act if it is in compliance with parallel policies established by its functional regulator in accord with the Gramm-Leach-Bliley Act. This important determination will enable regulators to avoid imposing needless duplication upon the Nation's financial services companies. I appreciate the opportunity to be here today and would be happy to answer any questions you may have.

[The prepared statement of H. Randy Lively can be found on page 119 in the appendix.]

Mr. HENSARLING. Thank you.

Mr. Bohannon, you are now recognized for 5 minutes.

STATEMENT OF MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT OF PUBLIC POLICY, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION

Mr. BOHANNON. Thank you, Mr. Chairman, members of the subcommittee. I appreciate this opportunity to appear before you today and testify on why we need a national framework for data security. As the principal trade association of the software and digital content industry, many of whose members are leaders in high tech, SIIA was one of the first voices urging Federal action to address the myriad and inconsistent State laws that have emerged since California's first went into effect in 2003. In working with all the stakeholders on this issue on both sides of the Capitol, we have argued that that national framework should be premised on the track record of the safeguards rule under the Gramm-Leach-Bliley Act, which many members and staff of this committee were instrumental in constructing. As a comprehensive yet adaptable model, the safeguards rule emphasizes ongoing security plans to prevent, and I emphasize prevent, what we all know are the pernicious effects of identity theft.

Our perspective on today's panel is probably a bit unique, and we especially want to thank Chairman Bachus for including us in today's panel and his leadership on so many issues of importance to our industry. While some of our members are regulated as financial

institutions under existing laws, most of the members are software, e-businesses, and information content companies that are subject to the jurisdiction of the Federal Trade Commission and its section 5 authority. It is the effect of H.R. 3997 on these companies that we ask the committee to carefully consider and work with us as the bill moves through this process. In our written statement—Mr. Chairman, if it has not been introduced in the record in full, I ask that it do so now—we note that H.R. 3997 is consistent with several of our key goals in achieving a national framework. In particular, it recognizes the need to address the conflicts in the more than 21 States that have already enacted laws. We also in our written statement offer several important improvements to make the bill more workable and effective, notably in the areas of streamlining the obligations on data security procedures, establishing a meaningful threshold for breach notification much along the lines recommended by the Federal Trade Commission, and ensuring a meaningful definition of sensitive personal information.

But I want to make clear that we urge this committee to continue its work on this important bill. We especially commend the cosponsors on both sides of the aisle for coming together to produce this product, and we ask this committee to work with other relevant committees so that, in the end, when the Congress does act, and we hope they do, there is a coherent national approach achieved by this Congress.

In the remaining time available to me, let me focus on one aspect of H.R. 3997, and that is the framework of the Fair Credit Reporting Act, a vitally important consumer protection statute. As a means for establishing an enforceable framework, we request the following should be carefully considered by the committee, as many of our members today are not today within its scope. First, as I pointed out earlier in my testimony, most of our members are right now subject to the FTC's enforcement authority under section 5, which is today building on the safeguards rule of the Gramm-Leach-Bliley Act. Through cases that are being brought now under section 5, the FTC has found a variety of unfair practices ranging from failure to implement appropriate security programs to deceptive security claims made by companies. We think the FTC is headed in the right direction on this, and we want to encourage them to continue the direction of the policy under section 5. However, while H.R. 3997 has dealt with a number of laws that already exist, it is our impression in the bill, and we believe that it leaves those companies that are currently subject to section 5 enforcement open to possibly duplicative and even contradictory requirements. As we read H.R. 3997, nothing in the bill addresses this potentially confusing enforcement action.

The second issue that we would like to work with the committee and the sponsors on is that H.R. 3997 defines a financial institution as essentially any company that maintains the Social Security numbers of its employees or maintains a taxpayer ID number of its customers. Just this morning, it was pointed out to me that it may also include any person maintaining or communicating information on an ongoing basis even if they are mere conduits or hosts.

We are deeply concerned that this definition extends the concept of financial institution well beyond that used to date and poten-

tially brings in a wide range of companies into the purview of the FCRA, which concerns, as you might imagine, a number of our members.

We also share the bill's goal and the cosponsors' goal of effectively dealing with the myriad of State laws. We are cognizant that a number of circuits are reviewing what in fact falls in the scope of the FCRA. We note, to date, no State enacting a data breach security law including those with safeguard provisions has limited the scope of its law to the financial sector or to specifically regulated financial information. This is especially true of first State law enacted in California.

Mr. Chairman, to ensure a coherent policy approach, we once again urge this committee to continue its work on this bill, and we also ask that this committee work with other relevant committees as this process unfolds. It is our sincere hope that all stakeholders working together will be able to enact legislation in this Congress. It is a high priority for our association. We appreciate the opportunity to appear before you today, and I will be glad to take any questions that you may have.

[The prepared statement of Mark Bohannon can be found on page 58 in the appendix.]

Mr. HENSARLING. Thank you.

Ms. Brill, you are now recognized for 5 minutes.

STATEMENT OF JULIE BRILL, ASSISTANT ATTORNEY GENERAL, STATE OF VERMONT

Ms. BRILL. Thank you very much.

Thank you, Chairman Bachus, Ranking Member Sanders, for inviting me here today. I am very pleased to speak here on behalf of the National Association of Attorneys General.

My name is Julie Brill, and I am an assistant attorney general for the State of Vermont. As has been mentioned by several members so far this morning, there have been 48 attorneys general out in the States who have written a letter to Congress calling on Congress to enact a strong Federal security breach notification law modeled on the 22 State laws that are already in existence. Unfortunately, I am here today to tell you that the AGs' believe that H.R. 3997 fails to meet the standards of a strong Federal law. I wouldn't call it an ugly child, as had been mentioned earlier, but this child is failing in school and needs significant remedial help.

First, the AGs call on a law that would have a standard for providing notice to consumers that would ensure the consumers would receive notice whenever there is unauthorized access of personal information. We do not believe there should be an additional requirement of actual harm or risk of harm, and there is a very simple reason for this. The breached entity simply does not, in the vast majority of cases, know what use will be made of the information that it has lost. It just doesn't know. If Congress does want to incorporate some sort of concept of harm or risk of harm then the AGs strongly believe that notice should be given unless there is no risk of harm. What that means in simple terms is that the benefit of the doubt should be given to the consumer and to notice. If the breached entity does not know what will happen with that informa-

tion that was lost or stolen, then notice should be given to consumers. Again, the benefit of the doubt going to the consumer.

H.R. 3997 fails to meet the attorneys generals' standards for providing notice. It imposes complex and high barriers to consumer notice. Many of the incidences, as was mentioned by Representative Frank earlier, that have been reported under the State laws to date would not be subject to notice under 3997. As had been mentioned by Representative Hensarling, it is important to promote competition in security systems. H.R. 3997 would stifle competition in security systems because it would stop information from flowing to consumers about the harm that is occurring, that businesses are not having secure systems, and consumers would not be able to choose companies based upon their security systems because they wouldn't be receiving notices. We believe H.R. 3997 would place many consumers at risk because they would be unable to protect themselves from potential harm. The notion that consumers will ignore warnings because they will be getting so many of them, frankly, we think that is a red herring. Our experience in the trenches of identity theft war is actually the opposite. That numerous notices that consumers have been receiving over the past year have served as an important educational tool for consumers. Consumers are now much more aware of the risks that having their information out there can pose to them, and they are starting to take precautions. Thus, this notion that numerous notices would be harmful, we believe, is just simply not true.

Second, the AGs want to see their ability to enforce any Federal law that is enacted, and we are disappointed to note that H.R. 3997 does not allow for State attorney general enforcement. This is rather inexplicable because H.R. 3997 uses the Fair Credit Reporting Act as its construct, and the rest of the Fair Credit Reporting Act is, as most people are aware, enforceable by the State attorneys general.

Third, with respect to preemption, it should be noted that we wouldn't be here, this committee would not be considering this issue if it were not for State laws that were on the books now that provided for notice going to consumers and made the public aware of the massive problems associated with security of information. We think that preemption is a mistake. H.R. 3997 has broad preemption not only of security breach notice laws but also has apparent preemption for security freeze laws. In fact, this committee and Congress just 2 years ago gave the States the freedom to enact State laws on breach notification and security freezes. If this committee and Congress cannot provide adequate protections to consumers, we respectfully request that this committee take no action at all. The States listened to you 2 years ago; we started to enact laws. We are protecting consumers, and we will continue to do so. In the event that the law you enact is not strong, we think we would be better off without any law. Thank very much.

[The prepared statement of Julie Brill can be found on page 64 in the appendix.]

Mr. HENSARLING. Thank you.

Mr. Hendricks, you are now recognized for 5 minutes.

STATEMENT OF EVAN HENDRICKS, PUBLISHER, PRIVACY TIMES

Mr. HENDRICKS. Thank you. I am Evans Hendricks. I am in my 25th year of publishing Privacy Times and the author of the book, Credit Scores and Credit Reports. The book describes how, in part, because of the leadership of this subcommittee and the committee and its counterpart in the Senate and because the constructive bipartisan approach taken by the members and the stakeholders willing to work together, in 2003, we passed important and complex legislation, the FACT Act, which represented a major step forward for consumers and improved protections for identity theft.

As a housekeeping matter, I need to mention in addition to the eight groups that have signed on to my testimony subsequent to me turning in the testimony, Consumer Action, the National Consumer League, identity consultant Maury Frank, and five additional groups have signed onto the legislation—excuse me, to my testimony. To get this very simple message to the committee, this bill would represent a serious weakening of current standards and represents a step backwards. There are children, and then there are pets. If you could sum it up that way, we would say this dog don't hunt.

In 2003, I testified before this subcommittee thanks to Chairwoman Kelly, who held the first breach hearing on the breaches of credit card data. At that time, I said I recommended that the subcommittee move legislation based on the California breach notification law. It is very important to understand that if you are going to have Federal law, you need to start from a high level of protection and preferably get out in front of the issue. Now things are more difficult when States have to move to protect their citizens because of Congress not being able to do it and get out in front of the issue. The Supreme Court has defined privacy. To begin with, both the common law and literal understandings of privacy encompass the individual's control of information concerning his or her person. If there is a breach, you lose control of the information. If you can't get access to your records, you lose control of the information. If you can't correct errors, you lose control of your information. On top of that, we had a hundred data breaches this year; 50 million people whose data has been potentially exposed which, by the way, is about the number of people that have signed up for the do not call list. Americans care about privacy. A month ago, the New York Times and the CBS News released a poll showing that 89 percent of the public was concerned about identity theft. More interesting was 3 percent were not concerned at all. I would like to interview those people and find out what's up. But more importantly, for today's purposes, they said this was a very bipartisan issue: 68 percent of conservatives and 69 percent of liberals would like to see the Government do more to address personal privacy issues. And that is why there is cutting edge companies like ING Direct and E-loan, financial services companies that we see are supporting stronger consumer protections for privacy. The problem with this bill, as luckily Julie Brill went first to give the more detailed analysis, it dramatically weakens breach notification standards through its harm trigger. It dangerously would weaken the very straightforward security standards of Gramm-Leach-Bliley. It

would preempt State laws and possibly preempt freeze laws without even using the word freeze. We need to go the other way and enact Federal freeze law based on the best State standards.

It is very silent on a very important issue. This year, we have had breaches of ChoicePoint and Lexis-Nexis and a great opportunity to move forward and extend FCRA style rights to the data brokers like ChoicePoint and Lexis-Nexis. The bill is silent on that. There is other legislation that would accomplish this.

I think basically privacy is nothing new; privacy is always challenged. You might have seen the Washington Post article from Sunday showing how national security letters are being used for sweeping investigations that include getting all sorts of transactional data on Americans, including their credit reports. That is why I think that we have to be very cautious in causing no harm and preferably would do something bold but given the problems we face and Americans' strong desire for privacy, we don't want to enact a law that can be characterized as the Titanic deck chair reorganization act. We need to really get out and move forward to protect Americans.

In considering this legislation, I think you have to keep in mind that privacy signifies the tension between individuals' desire for control over their information and large organizations' desires to use that information for their own purposes, whether it is business or governmental. I think you should remember that since consumer confidence and consumer spending is an important part of our economy and our future and that those people, the taxpayers that underwrite our Government, that when we come to close calls that we should tilt in favoring the individual's right to privacy.

Thank you very much.

[The prepared statement of Evan Hendricks can be found on page 86 in the appendix.]

Mr. HENSARLING. Thank you, Mr. Hendricks.

Last but not least, Mr. Kaufmann, you are recognized for 5 minutes.

STATEMENT OF KARL F. KAUFMANN, SIDLEY AUSTIN BROWN & WOOD LLP, ON BEHALF OF CHAMBER OF COMMERCE

Mr. KAUFMANN. Thank you. Good morning. Good morning to the chairman and ranking member of the subcommittee. I'm Karl Kaufmann, and I am an attorney here in the Washington, D.C., office of the law firm of Sidley Austin Brown & Wood. I am pleased to appear before you today on behalf of the United States Chamber of Commerce. The Chamber is the world's largest business federation representing more than 3 million companies of all sizes and across all sectors of the economy. Mr. Chairman, the Chamber supports your effort and the efforts of others on this subcommittee to develop legislation to protect the sensitive information of consumers. The Chamber believes the vast majority of companies who possess sensitive personal information take reasonable procedures to safeguard that information. However, it takes only a few mistakes by a few companies to damage consumer confidence in the ability of all companies to protect sensitive personal information. Therefore, we believe that Congress should require the companies have reasonable programs to safeguard consumers personal infor-

mation, and this concept is, in fact, a fundamental part of the Financial Data Protection Act.

The Chamber also believes it is appropriate for a company upon discovery of a data breach to notify its customers if their sensitive personal information has been subject to the breach. However, it is important that Congress require the notices only when the sensitive personal information is acquired by an unauthorized person in a manner that presents significant risk of harm to consumers. Otherwise, we believe the consumers may find these types of notices to be meaningless, and consumers may then begin to ignore such security breach notices. If this occurs, the goal of using these notices to notify customers of their rights and notify them of the breach is undermined. If breach notices are limited to circumstances when the consumer is at risk of harm, it is more likely the consumer will be aware it contains important information and that it should be read.

We applaud the fact that the sponsors of the Financial Data Protection Act agree with the Chamber's view on this key issue, and given some of the testimony, I would like to spend a little bit more time on this. It seems odd to require a notice be given to consumers just because there has been a data breach. I can imagine situations where a breach occurs, but, in fact, there is no way that the data could be misused. Perhaps it was a breach of numbers that are so-called disposable credit card numbers used for online shopping. Maybe it is information that is highly encrypted, password protected and has other protections that make it essentially unusable. It would be unusual to provide a consumer with a notice in that circumstance that says the information has been accessed, but don't worry; there is nothing that you can do about it because you are protected. The consumer is going to ask, why am I getting this notice if I'm not supposed to do anything? Our belief is consumers should get notice when they have actually something that they can do to protect themselves.

Perhaps most importantly, any law passed by Congress must establish a national uniform standard with respect to information security, consumer notification, and other related issues. The consumer protections envisioned by Congress will be undermined if States can establish different schemes pertaining to data security. The Chamber is pleased the Financial Protection Data Act includes provisions to provided for national uniformity. Again, this is another issue that has drawn some interest today, and I would like to go a little bit more in depth.

Providing a uniform national standard with respect to data security is an absolutely essential consumer protection. The proliferation of similar but ultimately different State laws with respect to information security issues is not in consumers' best interest. Varying notification standards can result in consumer confusion and inconsistent compliance with the law.

Furthermore, the net result is that the States that require the notices in the most instances with respect to data breach notification requirements will essentially set the national standard. Companies that operate in all 50 States cannot efficiently design compliance programs to take into account the differences among the 50 State laws. Therefore, those companies are more likely to establish

regimes under which they will find the most onerous State law and make that their standard. If they comply with that, they will comply with other State laws as well. The net result is we end up, again, perhaps with notices sent when they are not necessary, and that is a concept again that is included in this bill. And if people believe in the fact that consumers should be notified only when it is meaningful to that consumer, allowing for States to undermine that important protection does not seem to make a whole lot of sense.

Now having said that, as you can see, the Chamber supports many of the concepts addressed in the Financial Data Protection Act. We believe these concepts will provide a sound framework for strong consumer protections if they are properly implemented. We also understand that the legislation continues to evolve and that it may require additional refinement. Indeed, the discussion that happened this morning suggested that that is the case. The Chamber looks forward to continuing to work with you, Mr. Chairman, and others to continue to shape this complex bill as it moves through the legislative process. The Chamber appreciates the opportunity to present its views this morning, and I would be happy to answer any questions that you may have.

[The prepared statement of Karl F. Kaufmann can be found on page 113 in the appendix.]

Chairman BACHUS. Thank you.

At this time, we will ask the members to address the panel.

Mr. Hensarling, am I catching you off guard by asking you to go at this time.

Mr. HENSARLING. No more than usual, Mr. Chairman.

Chairman BACHUS. I just thought I would let you all go ahead because I am not sure how long we have got before we go to the floor.

Mr. HENSARLING. Mr. Kaufmann, since you are already warmed up, perhaps I will start with you. You may have heard in my opening statement I quoted Chairman Greenspan who said something along the lines that I cannot believe we need regulations to tell people how to make a profit. Can you tell me what your opinion is of the incentive structure that private companies have today to protect personal data?

Mr. KAUFMANN. The incentive structure is quite strong if you look at the market forces that are out there. Regardless of whether the direct consumer relationship, say, is a bank or whether you are a service provider, lets say a card processor, in any circumstance, you face significant penalties in the marketplace if you do not protect consumers' data. Your name ends up on the front page of the newspaper. Your stock drops, as you mentioned. And I can assure you that some of the folks at ChoicePoint and Card Systems have had better days than the day the data breach was announced. Not only that, but people in the market place pay attention. I can almost be certain that every card processor out there looked at what happened to Card Systems and said, I don't want to be that company. I can assure you a lot of the data management companies looked at ChoicePoint and said that can't happen to us, that will not happen to us, and we must make sure that that does not happen. So the market forces are there in virtually all aspects.

Mr. HENSARLING. In your testimony, you mentioned how important it is to come up with, for lack of a better term, permit me to be redundant, a very definitive definition of security breach. Can you tell us why it is so critical that the definition be sharp, solid, and what would happen if we created an overly broad definition of security breach?

Mr. KAUFMANN. If you end up with an overly broad definition, then you even up with situations where it may or may not be the fact the data has been accessed by somebody who is not authorized to access that information. We need to talk about a situation where somebody actually obtains the information; the fact that they may have hacked into a computer system and bragged to their friends about the fact they were able to hack in, but they in fact didn't take any information out, and there is no evidence to suggest they were there long enough to write any information down, suggest that that information is not going to be misused and, therefore, to send out a notice seems redundant and perhaps counterproductive. And so what we need to focus on are situations where the information is accessed in an unauthorized manner a way that can present significant harm to the consumer and that way they are notified and not in other circumstances.

Mr. HENSARLING. Let me share the wealth here. Mr. Ireland, a related question. Many financial institutions have stated that they feel that the interagency guidance strikes a correct balance with respect to the notice trigger when there is a likelihood of harm to the consumer. Do you believe that a national notifying standard similar to that is warranted and indeed strikes the right balance?

Mr. IRELAND. I do believe a national notification system that applies to all institutions that is basically the same standard or a similar standard to the banking agency guidance for notification is appropriate. I would point out that that guidance works with the benefit of a dialog between the banks and their bank examiners as to figuring out when a breach has occurred and if it requires notice. And as Mr. Kaufmann indicated and your prior questions indicated, in a statute that is going to be self-operative and not benefit from that dialog, you need a crisp standard that people will understand from the language of the statute so you might not use the same language, but the basic model I think is a sound model.

Mr. HENSARLING. Can you share with the committee your opinion on the interplay of the form and the frequency of consumer notifications and how that impacts their effectiveness?

Mr. IRELAND. Well, the problem is that information in terms of—what could be characterized as a security breach may or may not be due to foul play and I don't want to go into individual institutions' problems, but I have seen many circumstances where information has been moved from one institution to another so that they could—for competitive purposes—so that you could solicit customers, for example. And there is no risk of identity theft or account fraud. This bill goes to great lengths to make sure the customers who get notices open the notices and read them when the notices are important. If we inundate them with notices when they don't need them, they may read the first two or three where there is no issue and the fourth notice where they do need to check the credit report to see if identity theft is going on, they may simply

have failed to open because they think it is the same as the first three. That is the problem we are concerned about, and we think the system—the notices will be much more effective if they are targeted to those situations where consumers themselves need to act to deal with the problem.

Mr. HENSARLING. Thank you.

I am out of time, Mr. Chairman.

Chairman BACHUS. Thank you.

Mr. Sanders.

Mr. SANDERS. Thank you, Mr. Chairman.

Let me ask Ms. Brill a few questions, if I might. Ms. Brill, since 2003, the Fair Credit Reporting Act through FACT allowed States to create a right for consumers to impose a security freeze on their credit report. Do you believe that H.R. 3997 would reverse course and remove the ability of States to create a right to security freeze? Why is it important to have a security freeze right for consumers? What has been Vermont's experience with security freezes?

Ms. BRILL. Thank you.

The security freeze provisions that States have enacted since 2003 really did come out of FACT. FACT's preemption provisions did not specifically state that States were unable to enact freezes. California enacted the first one; now 12 States have security freeze laws on the books. These laws are highly protective of consumers who may be in an identity theft situation. It allows them to place a hold on their credit report so that no one can access the credit report unless the consumer authorizes that access, and it has been considered to be one of the strongest tools available to consumers to help prevent identity theft. I will be honest with you; I work in the trenches of the State legislature; I am not an inside-the-beltway person. And when we looked—

Mr. SANDERS. Montpelier is not quite Washington.

Ms. BRILL. No, no. But we looked at FACT. We looked at what we were allowed to do based on what this committee told us we were allowed to do, and so the States went out and said, okay, Congress did certain things to help protect consumers with respect to identity theft, we can do other things, and it would be very confusing and frankly I think disruptive of the State legislative process to now just 2 years later tell State legislators and the State AG's that they cannot enact security freeze provisions. And where this comes from, frankly, is the preemption provisions of 3007 are quite broad and would, I believe, or could possibly be interpreted to prevent States from enacting—

Mr. SANDERS. Let me just ask one more question. State attorney generals have always been able to enforce FACT. Do you believe State attorney generals should be able to enforce a notice of security breach law and why?

Ms. BRILL. Absolutely. We work very closely with the Federal Trade Commission, and we respect their work a tremendous amount. We worked together with them on all issues, telemarketing, credit reporting. Frankly, they don't have the manpower or person power to deal with all the security breaches that are out there. They need an additional cop on the beat, and the State AG's are that additional cop on the beat.

Mr. SANDERS. Let me ask you a third and last question. Would H.R. 3997 preempt States' ability to enact privacy laws under GLB? What has Vermont's experience been with respect to its opt-in law? Should Congress reverse course on the States on this issue?

Ms. BRILL. I do believe that 3997, if read broadly, if its preemption provisions are read broadly, would preempt the States from enacting opt-in rules and would run contrary to, again, what this committee and other committees have said in GLB in section 507, which specifically allowed States to enact opt-in laws. Vermont has an opt-in law with respect to privacy, with respect to information and sharing.

Mr. SANDERS. How many States have opt-in laws?

Ms. BRILL. I believe about four or five. Some of the States only have it with respect to certain types of information and others it is much broader. But I think again it would be disruptive to the State process. We have been working through that process; we have submitted our laws to the FTC; we have gotten clearance from the FTC that our law is satisfactory under 507 because it is more protective of consumers, and now to reverse course and say you can't do what we told you you could do just 6 years ago, again, I wouldn't even know what to begin to tell my State legislative committees.

Mr. SANDERS. The bottom line is taking States out of this process would be harmful to consumers.

Ms. BRILL. Absolutely. Congress, I think, works best when it enacts a strong floor and allows the States to do more to protect consumers.

Mr. SANDERS. I absolutely agree, and I think that is the most important point that can be made this morning.

Thank you very much, Mr. Chairman.

Thank you, Julie.

Chairman BACHUS. You still have 24 seconds left.

Mr. SANDERS. I will give it to you.

Chairman BACHUS. Mr. LaTourette.

Mr. LATOURETTE. Thank you, Mr. Chairman.

I guess I would throw this open to anybody on the panel that wants to respond to it, but it is on the issue of encryption. And a lot of people have been pushing this; primarily many of the larger national organizations have urged us to include it in the bill, a bright line exemption for entities that use high-level encryption on their data systems. Basically, there are some who are advocating, if you buy the latest, cutting-edge equipment for encryption software as set forth by a regulator and based on the National Institutes of Standards and Technology that you are free and clear of any notice obligations to consumers under the bill. While I believe that encryption should be a factor that a company looks at when assessing a breach, I am wondering, how would your institutions or how do you think many of the small community banks in places like I represent in northeastern Ohio would manage under a bright line test for encryption.

Ms. CALLARI. I can speak for our company. We are a community bank. We do use high level of encryption on our data. The issue remains when our customers' information goes to other merchants and vendors and data processors and knowing what kind of

encryption they use. The other challenge is, we can secure data as much as we want until there is another very smart hacker out there who can break that encryption. So I think encryption is going to safeguard to a certain extent but not always.

Mr. LATOURETTE. Yes, sir.

Mr. BOHANNON. I appreciate your question. From our industry's perspective and by way of background, I used to be the NIST chief legal advisor, so I am very familiar with their process and what they do. We certainly believe that encryption is a very important element in looking at the overall security program that an entity has, and from our perspective as representing a broader range of companies, we think it is useful.

In the context of specific legislation, let me leave you with the following three thoughts. We would be concerned if only encryption were ever mentioned. We believe it has got to be a range of practices appropriate to the circumstances. Encryption, redaction, truncation, access controls all need to be recognized.

Second, in the context of other bills we have actually urged, rather than it being a factor that it be a related element of whether that actual risk has actually occurred or not, that it be a more bright line determination than we believe is in H.R. 3997, but we think that that can be changed and adjusted in the bill.

The third issue is whether the standards issued by NIST are appropriate. I caution you—and I will be glad to provide the committee with more data on this—the standards done by NIST were done in the context of Government use. It is important to understand that. While there are important lessons and results from those tests, we need to recognize that they may not be entirely appropriate or recognize other viable tools that are out in the private sector, particularly encryption algorithms, that may be not be recognized by NIST.

Mr. LATOURETTE. Ms. Brill.

Ms. BRILL. Just very, very briefly, I will note that the OCC in its guidance in the interagency guidance does not allow for any exemption whatsoever with respect to encryption, and we find it very interesting that certain pieces of the OCC guidance are touted by industry as being quite helpful whereas other pieces, for instance, the fact it covers paper records as well as electronic records and again this encryption point are ignored.

Mr. LATOURETTE. Mr. Ireland.

Mr. IRELAND. I would point out in response in part to Ms. Brill's comment, most States include an encryption or bright line encryption exception without the benefits of a more refined definition of what that constitutes.

The advantage of including such a provision, not in lieu of current provisions in the bill but in addition to other considerations, such as redaction, would be that you would provide a financial incentive in terms of concern about notification costs to raise the level of encryption and protection of information. And that might be a positive thing. So the argument for it I think is the incentive it creates, recognizing, as I think has been said, that any encryption standard may not be 100 percent impenetrable.

Mr. LATOURETTE. Thank you very much.

Chairman BACHUS. Could I suggest that we—we have three more members, if each took 3 minutes. Start with Mrs. Maloney, and then we will go to Mr. Price. That way, Ms. Hooley, who is a sponsor of the bill, would have an opportunity. Unless we want to come back. But I am told it is going to be about 12, 12:45, so, Mrs. Maloney.

Mrs. MALONEY. I would like to ask Mr. Hendricks and Mrs. Callari or really any witness to respond. What do you think we should do to address the concern over foreign data processing and why should we allow consumers to prevent their personal data from being sent overseas?

This bill contains a requirement that foreign data processors agree to notify the U.S. company in case of breach of conduct and conduct a joint investigation of a possible breach.

But my question is, is that enough? Who can effectively enforce this provision? Who can police whether foreign data processors fulfill their contracts? And if a breach is defined to include, quote, a risk-based factor, that is, so that it isn't even a breach unless there is actual harm or significant risk of our actual harm, then aren't we allowing foreign entities to make a judgment that they have absolutely every incentive to make against the consumer's interests?

And, secondly, I would like to follow up on Ms. Brill, since we only have a short time. I would like any panelists to respond as to why AGs shouldn't be given the ability to enforce the notice of a breach of security, the point that she made of the resources not being there, that it is a huge problem in the country.

I thank you all for your very thoughtful testimony today. Thank you.

Mr. HENDRICKS. Thank you, Congresswoman, for that question. Congressman Markey has put the flag in the sand, saying people should be able to consent to having or withhold consent for having their information going overseas. We spent an hour and a half on this on a Brookings panel.

To me, outsourcing—if privacy is the steak, outsourcing is the sizzle because it really shows that there can be a loss in the custody and control; it attacks the integrity of the security chain of command in the use of the information, and there is a lot about the whole accountability and remedy if something goes wrong.

We have to—some of the bottom line things we have to make sure is to make sure that privacy protections and responsibilities are extended all the way down the chain of command. We have to make sure there is transparency so consumers always know when there is going to be outsourcing of data if we are going not going to require their consent first.

E-LOAN is the company that does it one way. They say, if you come to us during our regular business hours, we have our American staff process it. If you want the convenience of going after hours, they outsource that data. So through that transparency they are at least giving people a choice.

But, unfortunately, I think most companies are trying to hide the fact they are outsourcing.

Ms. CALLARI. I would like to add that, as a financial institution, we are regulated by GLBA, and we are already required to take re-

sponsibility for our customer information. So regardless where customer information resides, we are responsible.

We do not today outsource any of our customer information overseas. But it is also important to note that H.R. 3997 does mandate that third parties contractually agree to disclose any breaches.

Mr. KAUFMANN. Congresswoman, if I could take a minute to clear up what sounds to me like perhaps a misconception that once the data is sent to a company that is located overseas or an office that is located overseas that the U.S. law doesn't apply. In fact, the U.S. law does.

So just because a bank—let's say where a company chooses to use a processor in New York or chooses to use one in Canada does not mean they can say, well, we can evade U.S. law by sending this data to Canada. In fact, that is not the case. Regardless of whether we are talking about financial institutions or not, I think just principles of—principal and agency law suggests that if your agent—if your service provider misbehaves in a certain way, the principal—the company that use that agent will be held accountable, and so I just wanted to make that clarification.

Chairman BACHUS. All right. Thank you.

Ms. Hooley.

Ms. HOOLEY. Thank you, Mr. Chair.

I have just a couple questions. I will try to be brief. Let me start with Mr. Hendricks.

You note several—there are several things that you think are good about the bill. One of the things you are talking about is notification, and you would encourage the committee to expand credit monitoring from 6 months to a year. My question is, do you have any evidence that it stops ID theft or would prevent ID theft if it is monitored for a year versus 6 months?

The second question is, do you see anything in the notice that you would suggest that we add additional information? Is there anything missing in that notification?

Mr. HENDRICKS. Yes. First of all, on the credit monitoring, this is a moving—identity theft evolves, and no one has followed it more closely than you. Reflecting that fact is that the thieves are getting shrewder and shrewder and the shelf life of a social security number is basically for the life of the individual. So we are going to see more and more thieves are sitting on data to use it later, hoping that now people are no longer being careful. So in ChoicePoint they offered it for a year. A year seems like a reasonable period of time to get people started.

The monitoring is important because it gives you the notice. That is also why the credit freeze is important because it is that key moment when the credit reporting agency discloses your credit report to the application of the thief that that is what allows identity theft to take off.

Now your second question was about—

Ms. HOOLEY. It was about the notification. Do you see if there is something missing in that notification?

Mr. HENDRICKS. It would be nice if the notification could just be robust enough so that the entity could tell the individual as much they know about the breaches because what is happening, first of all, I think the standard in the State laws is working fairly well.

And out of all these cases, I have not seen a trivial notice go out. But in hearing from people and going through each case by case, you see that a lot of individuals get the notice and the company actually knows more, but they don't include in the notice. So it only comes out in subsequent news stories further explaining what was at stake.

If we want to encourage companies to give as much information as they can, that helps consumers make judgments about what are the risks here.

Ms. HOOLEY. Thank you.

A very quick question for Ms. Brill. Thank you very much for coming today.

In your testimony, you stated there should be no fraud monitoring exception, especially with respect to compromised information relating to debt card, bank account, or other noncredit account information.

My question is, what do you mean by fraud monitoring? And are you referring to required credit monitoring services when a consumer is placed at risk of ID theft? Because I would note the bill does require business to monitor for fraud using a neutral network or a similar system.

And if yes, why should business be required to provide 6 months of free credit monitoring service when the information that is lost would not lead to a threat of ID theft? If the only change they needed—say, they just had to give you a new number or new card. Why would you require them to do 6 months of monitoring for that purpose?

Then the second question—I will get it all out at once—the second question we talked about freezes, a lot of you talked about freezes. Do you think it is better to have—through Federal legislation to do a freeze or let States do a freeze?

Ms. BRILL. I will take those.

Should I continue? Should I respond to that?

Ms. HOOLEY. Sure. We have 5 minutes.

Chairman BACHUS. We will end these questions, but we will come back if Mr. Hinojosa and Green want to come back.

They will pass.

Ms. BRILL. So I will go ahead and respond now.

Chairman BACHUS. And then we will let Mr. Hinojosa ask a question.

Ms. BRILL. Thank you very much.

With respect to fraud monitoring, our concern did deal with a neural network issue as you pointed out. It wasn't so much relating to the credit monitoring services that were provided.

But we are concerned that a blanket exception for a company that does fraud monitoring is not granular enough. It doesn't really go into the details of how good is the system and whether or not, in fact, an exception should be given just on a blanket basis. And we see some of the same problems in the language of 3997.

With respect to a freeze, the AG's letter does spell out what we think would be a robust, good Federal freeze law. Again, if Congress were to enact a Federal freeze that contains all of those provisions, we think that would be very helpful. If Congress cannot enact a law that contains all those provisions, then leave it to the

States, because the States are doing a pretty good job. Twelve are in place so far, and more will come on line undoubtedly in the future.

Chairman BACHUS. Thank you.

Mr. Hinojosa.

Mr. HINOJOSA. Thank you, Mr. Chairman. I will be brief, but I do want to say I have a great deal of interest in this consumer report and what comes out of our committee.

I understand that many people do not distinguish between data breaches and identity theft and that not all data breaches lead to identity theft. I also understand why many are calling for a uniform national standard governing data brokers and the services they provide, and I will support that. I support the idea of such uniform standards only if the statute we enact first and foremost protects the consumers and grants them as many avenues of recourse as possible if their identity is stolen as a result of a data breach.

Under the Texas credit freeze statute, if I felt my identity had been compromised, I would simply send a letter by certified mail to the consumer reporting agency requesting that it place a security freeze on my consumer file. The consumer reporting agency would have 5 business days to comply with my request. The agency would be required to send me an explanation of how to go about placing, removing, and temporarily lifting my security freeze. So if I were to decide to lift that freeze, the consumer reporting agency would have to remove the freeze no later than the third business day after it received my request.

All in all, I think that Texas has a much tougher requirement than what is contained in the proposed law.

All this to say, Mr. Chairman, that I support a uniform standard governing the protection of sensitive consumer information and the duty to provide notice when such information is compromised. I believe that H.R. 3997 falls short of that goal. I would hope that we can fine tune the bill's definition of several words as follows: breach, sensitive personal information, and the Gramm-Leach-Bliley provision.

Mr. Chairman, I wish we had more time today to ask more questions. I believe that there is room to improve this bill, and I fully intend to be part of the discussion. I hope that this committee holds additional hearings prior to markup. Too much is at stake not to proceed deliberaltely.

With that, Mr. Chairman, I am going to close and ask that the Texas statute on data breaches and account freezes be made part of the record.

Chairman BACHUS. Sure. In fact, the Chair notes that some members may have additional questions for the panel and may wish to submit them to the panel in writing. Without objection the hearing record will be held open for 30 days for members to submit written questions to the witnesses and place their responses in the record and, also, if they have their opening statement, they are free to submit that.

I appreciate the panelists' attendance today. As I said at the start of this hearing, we expect this to be a long process. I am submitting testimony from four witnesses that we didn't have room for

on the panel: ID Analytics Corporation, Mortgage Bankers Association, ARMA International, and the National Business Coalition of E-commerce and Privacy. In addition to your testimony, we will introduce those.

I would like to close by saying we have two new staffers on the panel, and I would like to welcome them. They have worked very hard on this hearing, Danielle English, who is with Mr. Boehner and Ms. Biggert previous to joining our subcommittee; and Emily Pfeiffer, who is with Mr. Castle, our Chairman Castle. We welcome them to the staff and compliment their good work.

So, with that, the hearing is closed, and the record will be held open for 30 days.

Thank you.

[Whereupon, at 12:14 p.m., the subcommittee was adjourned.]

A P P E N D I X

November 9, 2005

Statement of
Chairman Michael G. Oxley
Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit
H.R. 3997, the Financial Data Protection Act
November 9, 2005

This morning, the Committee meets to hear from a number of leading business and consumer groups on H.R. 3997, the Financial Data Protection Act. This bipartisan bill is the product of the hard work and leadership of Representatives LaTourette, Hooley, Castle, Pryce and Mr. Moore of Kansas. I congratulate them on their accomplishment and also thank the Subcommittee Chair and Ranking Member for spotlighting this issue in their hearings. This issue will be a priority for the Committee when we return next year, and I look forward to working with the sponsors as well as the Subcommittee Chairman and the Ranking Member.

In recent years, criminals in the United States and abroad have become increasingly inventive in finding ways to access and exploit information systems in order to commit identity theft. According to a Federal Trade Commission estimate, over ten million Americans are victimized by identity thieves each year, costing consumers and businesses over $55 billion per year.

Several recent high-profile security breaches have focused public attention as never before on the vulnerabilities of companies' data security systems. This year alone, we have seen nearly 75 breaches impacting over 50 million Americans. As a result of these numerous breaches, Congress needs to review how information is handled and what happens when it's mishandled.

The Financial Services Committee has worked tirelessly over the past several years to identify and enact solutions to improve data security protections. In 1999, many of the senior members of this Committee helped enact the first data security laws in the Gramm-Leach-Bliley Act applying to financial firms. In 2003, the gentleman from Alabama, Mr Bachus, led the Committee in expanding on this effort by securing the passage of the Fair and Accurate Credit Transactions Act, or FACT Act, which greatly expanded consumer identity theft protections.

A number of other committees in the House and in the Senate are also working on legislation to address data security protections. This Committee must do its due diligence by producing legislation that sets national protection for consumers and supports the financial services marketplace.

We can build on the work we did on the FACT ACT to achieve a unified product coming from this Committee. We have a great deal of expertise on this Committee on these issues, and I expect that our legislation will be a significant portion of any final House product. We seek to achieve a uniform national standard that protects consumers to a greater overall degree than they are protected now.

H.R. 3997 requires all businesses with sensitive information on consumers to adopt data security policies and procedures, investigate data security breaches, make uniform notification and provide mitigation to consumers where there is a likelihood of harm to the consumer. I applaud the bipartisan cosponsors for putting together a balanced, fair, and reasonable approach for our Committee, and look forward to further consideration of this legislation going forward.

###

STATEMENT OF REPRESENTATIVE GARY L. ACKERMAN
HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

HEARING ON H.R. 3997,
THE "FINANCIAL DATA PROTECTION ACT OF 2005."

WEDNESDAY, NOVEMER 9, 2005

Thank you very much Chairman Bachus. I want to thank you and Ranking Member Sanders for holding this hearing. With the long list of security breaches this past year involving banks, data brokers, and other financial institutions, I believe Congress must act quickly in order to protect the identities of the countless Americans who are clearly at risk.

I am concerned, however, that, in our haste to respond, we may be focusing on the wrong piece of legislation. Compared with several other bills addressing this issue, H.R. 3997, the Financial Data Protection Act, does too little to improve the protection of consumer data and may in fact weaken both the federal and state protections that are currently in place.

We need to ensure that the legislation we forward to the House is at least as strong as the best state laws already on the books. I would note in particular California's law that, since enactment, has successfully forced companies nationwide to promptly notify consumers about data breaches.

In addressing this issue, great care and precision in defining terms is vital. For example, a "security breach" should not be defined narrowly and require "financial fraud" as a precursor to triggering protections. Rather, as recommended in a letter last month by the National Association of Attorneys General, which has been submitted for the record, a "security breach" should be broadly defined to include *any* unauthorized access to personal information, and increase the level of protection that we currently provide to consumers.

And, in keeping with the common habit of respecting federalism only when convenient, H.R. 3997 would prevent its security requirements from being imposed under state laws. Instead, legislation passed out of this Committee should enable States to enforce security breach notifications laws in either state or federal court to ensure American consumers enjoy the greatest possible protection of their credit and identities.

Finally, I believe we need to maintain and extend the standards of Gramm-Leach-Bliley and the Fair Credit Reporting Act in data security legislation, rather than replacing these statues with a lower set of standards for protecting the confidentiality of consumer information.

I want to thank you again, Mr. Chairman, for holding this hearing today.

Congressman Joe Baca
Opening Statement
Subcommittee on Financial Institutions and Consumer Credit
A hearing on "H.R. 3997, Financial Data Protection Act of 2005"
November 9, 2005

Thank you, Mr. Chairman. I would also like to thank the witnesses for being here today.

In 2005 there have been at least 118 disclosed incidents of data security breaches, potentially affecting nearly 57 million individuals.

These breaches have weakened consumer confidence as recent surveys show. A CBS News/ New York Times Poll in September indicated that nearly nine in ten Americans are concerned about the theft of their personal and financial information. As a result, according to a survey by Consumers Union, twenty five percent of Internet users have stopped making purchases online. Of those who do shop online, twenty nine percent have cut back because of concerns about identity theft.

The American people have a right to be protected against identity theft. While the bill before this committee recognizes the need for stronger consumer safeguards, I am very concerned that it preempts strong state laws that have been effectively working to address this problem.

When Congress passed the Gramm-Leach-Bliley Act in 1999, it specifically invited the states to enact stronger financial privacy protections than those contained in the federal law. To date, my state of California has paved the way in pioneering the most effective data security solutions.

In fact, California enacted the first security breach notification law in the nation in 2003. Since then, at least 21 additional states have enacted similar statutes. California was also among the first – if not the first – to require individual consent before sharing financial information with third parties and to allow people to freeze their credit. Several states have also followed suit.

We need a strong national standard that protects personal information and notifies consumers when their data is breached by unauthorized users. By preempting state laws that are providing stronger safeguards, this bill effectively ignores the important lessons we've learned. Federal law should build upon these lessons and not weaken strong state standards for the sake of uniformity.

HR 3997 sends a message to the American people that their demands for stronger privacy protections have fallen on deaf ears. It gives consumers very little control over how their personal information is used by financial institutions and leaves consumers vulnerable to identity theft, aggressive marketing practices and fraud. Our constituents deserve better, and I hope that members on this committee agree to work in a bipartisan manner to address these concerns.

Thank you, Mr. Chairman.

OPENING STATEMENT OF CHAIRMAN SPENCER BACHUS
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"H.R. 3997, THE FINANCIAL DATA PROTECTION ACT OF 2005"
NOVEMBER 9, 2005

Good morning. The Subcommittee will come to order. Today's hearing on H.R. 3997, the Financial Data Protection Act of 2005 is the fourth Committee hearing this year on improving data security for consumers. During the past several years, this Committee has passed various pieces of legislation addressing aspects of the identity theft issue. Most importantly, the Fair and Accurate Transactions Act or FACT Act contained provisions not only preventing identity theft but giving victims added protections and remedies. This morning, we will consider data security legislation, which will give Americans further consumer protections against credit card fraud, identity theft and release of confidential information.

Introduced by Mr. LaTourette, Ms. Hooley, Mr. Castle, Ms. Pryce and Mr. Moore, H.R. 3997 seeks to expand the data safeguards requirements of the Gramm-Leach-Bliley Act and Fair Credit Reporting Act more broadly by establishing uniform standards for all businesses that possess or maintain sensitive financial account or identity information about consumers. H.R. 3997 would prevent data breaches by mandating a strong national standard for the protection of sensitive information on consumers; require institutions to notify consumers of data security breaches involving sensitive information that might be used to commit financial fraud against them; and require institutions to provide consumers with a free six-month nationwide credit monitoring service upon notification of a breach.

Over the last several months, there have been numerous news reports describing potentially serious breaches of information security. These breaches have generally involved sensitive personal information, such as individual names plus Social Security numbers or payment card information. Although the reports of subsequent fraud associated with these breaches have been relatively low, protecting consumers after such data breaches obviously remains a primary concern. Furthermore, data breaches, even if relatively uncommon and limited in scope, undermine consumer confidence more broadly. For instance, surveys suggest the growth of on-line commerce is restrained due to fears about information security.

Our fundamental goal is to ensure that companies protect sensitive consumer information to avoid potential security breaches. Unfortunately, no data protection program is perfect. Therefore, we need to make sure that companies take reasonable steps to protect consumers in the event that there is a breach. This morning we will have a discussion about providing notices to consumers who are affected by a data breach in addition to other ways consumer harm can be mitigated. These notices should only be sent out when appropriate so as to avoid over-notification of consumers. In addition, Congress should establish a national uniform standard to protect all Americans from data breaches. Lastly, data security legislation should distinguish between identity theft and credit card fraud. H.R. 3997 goes a long way toward achieving those objectives, and I look forward to moving this bill forward in the near future.

As I mentioned earlier, the sponsors of H.R. 3997 should be commended for drafting bipartisan data security legislation. I also want to recognize the work of

Ms. Bean, Mr. Frank and Mr. Davis on H.R. 3140, the Consumer Data Security and Notification Act of 2005. Like them, I think the time is ripe for Congress to act on data security legislation and will work with the sponsors of H.R. 3997, H.R. 3140 and other members of this subcommittee on this important legislative initiative.

Let me close by welcoming our panel of witnesses. We have with us today Oliver I. Ireland, Partner, Morrison & Foerster LLP, on behalf of the Financial Services Coordinating Council; Josie Callari, Senior Vice President, Astoria Federal S&L Association and Chairman of the America's Community Bankers Electronic Banking and Payment Systems Committee, on behalf of America's Community Bankers; H. Randy Lively, President & CEO of the American Financial Services Association; Mark Bohannon, General Counsel and Senior Vice President Public Policy of the Software and Information Industry Association; Julie Brill, Assistant Attorney General for the State of Vermont; Evan Hendricks, Publisher of the Privacy Times and Karl F. Kaufmann, Sidley Austin Brown & Wood LLP, on behalf of the Chamber of Commerce. I look forward to hearing from the witnesses and thank them for taking time from their schedules to join us.

I am now pleased to recognize the Ranking Member, Mr. Sanders, for any opening statement that he would like to make.

Opening Statement of U.S. Representative Judy Biggert (R-IL)
Financial Services Financial Institutions Subcommittee
Hearing on "H.R. 3997, Financial Data Protection Act of 2005"
Wednesday, November 9, 2005
10:00 a.m.

I would like to thank Chairman Bachus for holding this hearing today.

The Chairman and many members of this Subcommittee are no strangers to consumer information protection. This Committee has done an exceptional job in recent years, under the leadership of former Chairman Leach, Chairman Oxley and Subcommittee Chairman Bachus, to ensure that consumers are notified about their information privacy rights. In addition, we have worked hard to make sure that consumers have recourse with law enforcement authorities and credit reporting agencies in the event that they are victims of identity theft and need to set their credit record straight.

This Committee has produced exceptional legislation in this regard, including Gramm-Leach-Bliley, the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). However, due to recent data breaches, we have returned to the hearing room to, again, enhance consumer protections.

In February, the Federal Trade Commission issued a report indicating that the number of identity theft victims has only risen since 2002. In 2004, my home state of Illinois made the FTC's top ten list of identity theft victims for the third year in a row. In fact, two of the top five cities in Illinois with the highest number of identity theft victims are located in my district. But data breach and identity theft are issues not unique to Illinoisans. Breaches affect constituents in every corner of this country.

This year, I have worked with members of the Financial and Economic Literacy Caucus to educate consumers about identity theft. We should continue such financial education outreach, but we should also make sure that consumers' financial information is protected and that consumers are alerted in the event that their information is compromised.

I believe that the "Financial Data Protection Act of 2005" is a step in the right direction, and that is why I am signing on as a cosponsor of the bill today. While elements of the bill could be strengthened, the overall bill promises to provide a common-sense approach to tackling data breach issues. I commend Congressmen LaTourette, Castle, Pryce, Hooley, and Moore for introducing the bill. I look forward to working with the members of this Committee to iron out the details and produce a finished product in the near future. I welcome suggestions for strengthening the bill from today's witnesses.

STATEMENT OF THE HONORABLE WM. LACY CLAY
Before
The Subcommittee on Financial Institutions and Consumer Credit
"Financial Data Protection Act of 2005"
November 9, 2005

Good morning Chairman Bacchus, Ranking Member Kanjorski, Member of the Committee and Witnesses. I thank you Mr. Chairman for bringing this important legislation before the committee.

We have a crisis with security breaches of personal/financial data of American consumers. We have had corporate data security breaches that have compromised the financial security of over fifty million consumers. And this is a conservative estimate as there have been many breaches unreported. This is a national problem that must be addressed and safeguards put in place post haste to combat this growing cancer in our economy. Identity theft is an issue that adversely affects all of the population; that includes members of my staff in recent months.

I consider all data security breaches to be harmful. There is not a requirement on data thieves that they use the stolen information in a set period of time. Let us hope that the future does do reveal use of various stolen data that has not manifested as of yet.

I applaud the financial industry for the timelier reporting of these breaches over the last few months. It still is not quite what I would like to see or what is needed, but is a big step in the right direction.

I support H.R. 3997 and am confident that we can perfect this legislation and get it through to the Senate in a short time.

I yield back the balance of my time and look forward to the questioning of the witnesses.

Statement of the Honorable Harold Ford
Subcommittee on Financial Institutions and Consumer Credit
Hearing on HR 3997, the "Financial Data Protection Act of 2005"
November 9, 2005

Thank you Chairman Bachus and Ranking Member Sanders for holding this hearing which gives us the opportunity to discuss the prevalence of data breaches and what the Financial Data Protection Act can do to protect private consumer and business information.

I would also like to thank the witnesses for appearing before the Committee this morning on this increasingly important issue.

Data Security is important for everyone, especially in a world where technology allows someone at the touch of button to access a person's records. With that being said, it is not comforting at all that the New York Times reports that it has been a bad year for data security. The Privacy Rights Clearinghouse, a consumer advocacy group in San Diego, reports at least 80 data breaches since February, involving personal information of more than 50 million people across the nation. In 2003, 2,782 Tennesseans filed identify theft complaints in TN, and that number is only on the rise. In my district alone, National Bank and Commerce have had to deal with data security issues as part of their merger with Sun Trust. Sun Trust and a few other financial institutions had to reissue debit cards because of a security breach at a retailer. Even the United States government is dealing with data breaches of their own. The off-site data storage company for the House, Iron Mountain lost tapes in transit and in August, the Air Force reported a data breach by a hacker who may have gained access to a military management database and personal information on 33,000 officers.

With more and more sensitive information becoming apart of the everyday exchange of records among businesses, it is understandable that consumers are increasingly concerned about that information landing in the wrong hands. The Federal Trade Commission now estimates that 10 million Americans fall victim to identify theft each year, costing consumers and businesses more than $55 billion per year. Now is the time to have a meaningful discussion about comprehensive data security requirements. Congress has taken a good first step in protecting certain types of information and enacting requirements for different industries but that is not nearly enough. Now is the time for the industry to protect consumers from all data breaches and to provide adequate notification and assistance in the event sensitive information is stolen. I understand that there are differing opinions on what a national uniform standard should look like, and how consumers should be notified. I think it is important to remember that these are the key details in developing an effective response to the struggle consumers and businesses are dealing with everyday.

I welcome the testimony of the witnesses and the comments of my colleagues on this manner.

Opening statement on data protection hearing
Congressman Luis V. Gutierrez
November 9, 2005

Good morning. I want to thank Chairman Bachus for calling this hearing on the important topic of financial data security.

In July, Chairwoman Kelly and I held a hearing entitled, "Credit Card Data Processing: How Secure Is It?" I think the answer to that question was pretty clearly, "not secure enough." That hearing, like today's, benefitted from the testimony of Mr. Evan Hendricks, whose quarter-century of expertise on privacy issues has proved invaluable to this committee, and I'm certain his observations will be helpful today.

I have had a long standing interest in this subject dating from our work on the Gramm-Leach-Bliley Act. In 2003, I served as a conferee on the FACT act, which dealt with similar issues. In March of this year, I coauthored a bill with Congresswoman Melissa Bean on this issue, and I am proud to be an original cosponsor of the bill subsequently introduced by Representatives Bean and Artur Davis. I believe that the Bean-Davis bill provides a much better answer to this problem than HR 3997, and I hope that when we proceed to markup, our final product more closely resembles the Bean-Davis legislation.

It is my hope that we report out a bill that would require companies to notify consumers whenever their personal or financial data information has been compromised. Our legislation should further assist identity-theft victims by also requiring credit bureaus to be notified and to place a fraud alert or freeze on all compromised accounts. Companies responsible for breaches should be required to cover all costs associated with credit freezes or fraud alerts for at least one year after the breach. The legislation should also create a private right of action so people have a remedy when they are damaged by breaches, and it should restrict the uses of Social Security numbers as identifiers.

Finally, what we enact should be a floor, rather than a ceiling, ensuring that states can continue to innovate in this area.

It is important to note that we would not even be here today if the California legislature had not passed its law requiring consumers to be notified about data breaches. Because California consumers were notified when breaches occurred, the press picked up the story, and we began to understand the scope of the problem. A number of other states have followed California's lead, including my home state of Illinois, which has a very strong law in place. I would find it hard to support any bill that preempts or is weaker than the standards set by Illinois. I urge my colleagues to avoid a case of fair weather federalism on this issue. State legislatures have long functioned as "incubators of innovation" because they have been able to act quickly and creatively to respond to changes in the marketplace. Frequently, their excellent product proves its merit beyond its borders and becomes the basis for a change in federal law. I am deeply troubled that HR 3997 could stifle this innovation, and weaken existing state and federal protections.

Similarly, we must ensure that our final product allows state Attorneys General enforcement authority along with federal entities. Consumers would suffer from the removal of the state Attorneys General and other state "cops on the beat." Finally, it is an issue of accountability. Very few consumers would ever figure out what federal agency to call if they were victimized, but most consumers know (and vote for) his or her state Attorney General and can ensure that that officeholder is held accountable. I look forward to hearing the testimony of the witnesses and to working with my colleagues to craft strong legislation that still permits the states to provide additional protections. Thank you. I yield back the balance of my time.

OPENING REMARKS OF THE HONORABLE RUBEN HINOJOSA
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS. CONSUMER CREDIT
COMMITTEE ON FINANCIAL SERVICES
H.R. 3997, THE "FINANCIAL DATA PROTECTION ACT OF 2005"

Chairman Bachus and Ranking Member Sanders,

I want to express my sincere appreciation for you holding this important and timely hearing today. It is my hope that this Subcommittee and the Full Committee will consider holding additional hearings on the legislation before we proceed to markup. Perhaps today's hearing will allow us to discuss related legislation that has been referred to this Committee.

If not, I would ask that additional hearings, or perhaps a roundtable, be held to compare and contrast HR 3997 with other data security legislation before this Committee as well as some of the different state laws enacted to protect data from being breached and possibly used to steal a person's identity.

I make this request because the Texas statute addressing identity theft is more stringent than the legislation that we are discussing here today. Is the federal government really taking this issue seriously when states are passing laws that are more rigorous?

I understand that many people do not distinguish between data breaches and identity theft, and that not all data breaches lead to identity theft.

I also understand why many are calling for a uniform national standard governing data brokers and the services they provide. I support the idea of such uniform standards, but only if the statute we enact first and foremost protects the consumers and grants them as many avenues of recourse as possible if their identity is stolen as a result of a data breach.

Under the Texas statute, if I felt my identity had been compromised, I would simply send a letter by certified mail to the consumer reporting agency requesting that it place a security freeze on my consumer file. The consumer reporting agency would have five business days to comply with my request. The agency would be required to send me an explanation of how to go about placing, removing, and temporarily lifting my security freeze.

If I were to decide to lift the freeze, the consumer reporting agency would have to remove the freeze no later than the third business day after it received my request. I would be able to make my request to lift the freeze in writing via certified mail or by telephone using certain identifiers. I believe that it is necessary to note that the Texas statute permits the consumer reporting agencies to charge consumers for the cost of the freeze up to a designated cap.

Therefore, I do not believe that the Texas statute constitutes an unfunded mandate.

Mr. Chairman, there is much more to the Texas statute, but my time is limited. Therefore, I ask unanimous consent to insert into the official hearing record Chapter 20 of the Texas Business & Commerce Code; Regulation of Consumer Credit Reporting Agencies; Definitions; 20.1.

All this to say Mr. Chairman that although I support a uniform standard governing the protection of sensitive consumer information and the duty to provide notice when such information is compromised, I believe that HR 3997 falls short of that goal. I would hope that we can fine tune the bill's definition of "breach," "sensitive personal information," the Gramm-Leach-Bliley provision and others to ensure that we protect consumers as much as possible.

Texas has enacted a very tough, pro-consumer identity theft statute, and I feel that this committee must do the same, if not more, to protect and represent our constituents.

Having said that, I yield back the remainder of my time.

Congresswoman Barbara Lee
Talking Points & Questions for DIMP Export-Import Bank Hearing
November 10, 2005

Madame Chairwoman, let me first begin by thanking you and the Ranking Member for organizing this timely and important hearing as we begin laying the groundwork to re-authorize the Charter for the Export-Import bank.

I believe that it is critical for Congress and this committee to conduct these oversight hearings on a periodic basis in order to maintain our system of checks and balances with the executive branch. Far too often in the last five years we have shirked our responsibility as a body to conduct proper oversight on a range of issues important to the American public, which is again why I appreciate the bipartisan nature of this hearing.

Four years ago we came together in a bipartisan manner to review and re-authorize the charter of the Export-Import bank, and to assess its performance in accomplishing its mission.

We found that the bank was not focusing enough on reaching out to small businesses, particularly minority and women owned businesses, and that the Ex-Im was not doing enough work in Sub-Saharan Africa.

In re-authorizing Ex-Im's current charter we required that the bank provide 20 percent of its loans (measured in dollar terms) to small businesses. Since 2002, the bank has yet to achieve this requirement.

We also required Ex-Im to expand its outreach to minority and women owned businesses. Although the bank claims that transactions in this area have increased by 36 percent since 2005, these transactions still represent less than 10 percent of Ex-Im's total authorizations.

Meanwhile since 2002 the bank's total number of transactions in Sub-Saharan Africa and the overall dollar value of those transactions have declined.

Clearly there is some sort of disconnect between what Congress would like the Export-Import bank to focus on, and what it is actually doing. I hope that the testimony today may shed some light on these two issues.

Thank you and I yield back.

Software & Information Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

Prepared Statement of

Mark Bohannon
General Counsel & Senior Vice President

Software & Information Industry Association (SIIA)

HR 3997,

The "Financial Data Protection Act of 2005"

Before the
Subcommittee on Financial Institutions
And Consumer Credit

U.S. House of Representatives

November 9, 2005

PREPARED STATEMENT

Mr. Chairman, members of the Subcommittee, I appreciate this opportunity to appear before you today and testify on the fundamental need to establish a national framework for data security, including effective and meaningful security plans and breach notification.

As the principal trade association of the software and digital information industry,[1] SIIA was one of the first voices urging federal action to address the myriad of state laws that have emerged since California's first went into effect in 2003. We are working with all relevant Committees on both sides of the Capitol to accomplish this objective.

In our view, a national framework should be premised on the track record of the "Safeguards Rule" under the Gramm-Leach-Bliley Act, which many Members and staff of this Committee were instrumental in constructing. As both a comprehensive, yet adaptable model, the "Safeguards Rule" emphasizes on-going security plans to combat the pernicious effects of identity theft, giving consumers uniform protection that can be effectively enforced by authorities and implemented efficiently by business. Within this existing framework, notification is one additional tool – but not the silver bullet – that can advance the goals of the Safeguards Rule.

Our review of HR 3997 is premised on two considerations: (1) While some of our members are regulated as "financial institutions" under existing laws, most of SIIA's members are software companies, ebusinesses, and information service companies, as well as electronics companies, that are subject to the jurisdiction of the Federal Trade Commission (FTC) and its Section 5 authority. It is the effect of HR 3997 on these companies that we ask the Committee to consider as the bill moves through the process. (2) We review each legislative proposal through a set of principles that we believe are central to a meaningful national framework.

In a number of respects, it is clear that the goals and objectives of HR 3997 are consistent with these general principles, some of which we highlight below. While we believe that there are important improvements that can be made to make the bill more workable and effective,[2] we urge the Committee to continue its work on this bill and to work with other relevant Committees to ensure that a coherent national approach is achieved in this Congress.

---

[1] The more than 700 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

[2] We will be providing the Committee with more detailed suggestions following the hearing.

For example, HR 3997 shares one of our key principles: to create a meaningful national data protection framework. With more than twenty-one (21) states having already enacted data security and breach notification laws (most in this current calendar year), a national standard is needed to avoid confusion to consumers, businesses and the appropriate enforcement authorities. We believe the bill can be improved by streamlining the obligations on data security policies and procedures along the lines of the existing "Safeguards" provisions of GLBA so as not to over proscribe the steps and requirements an entity must take. We also appreciate the changes made to HR 3997, prior to introduction, to clarify the roles of 3rd parties in the event of breaches. However, we would suggest further clarification that notices – in order to be effective and ensure consumer awareness and responsiveness – must come from the entity with whom the consumer has the direct relationship, while permitting, as the bill does, the allocation of costs and logistical responsibilities through contracts.

On the critical issue of establishing a meaningful threshold for breach notification, there is a growing consensus to avoid over-notification to consumers. In testimony before Congress, four of the five FTC Commissioners, including the Chair, urged that the meaningful standard should be where a breach "creates a significant risk of identity theft." Our review of HR 3997 finds that the bill includes several thresholds. Taken together, these are likely to lead to confusion. Confusion leads to over notification. To avoid this result, as well as avoid consumer frustration and the possibility of unintended consequences (like increased incidences of phishing as a result of notification), SIIA strongly urges that:

- the threshold should be clearly established upfront and be based on the reasonable belief of an entity that owns or maintains sensitive financial personal information that a breach of such data in electronic form has occurred and there is a significant risk of identify theft; and

- the bill should specify that where data is collected, maintained or used with established information security practices, such as encryption, access controls, redaction or truncation, no such significant risk exists. This approach both facilitates the adoption of good practices, while not over proscribing the means to get there.

In discussions with all Committees, SIIA has recommended clear instructions to regulators, including the FTC, not to impose technology mandates. Virtually every proposal now before Congress has recognized this need, and we hope the Committee will include a similar provision in HR 3997. This language should not preclude steps to encourage voluntary adoption of security best practices.

Central to an effective national framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. We continue to review how the definition of "sensitive financial personal information" that includes both sensitive *financial account* information and sensitive *financial identity* information will in practice work. We note that "identity" information includes some items (such as taxpayer ID number) that are generally available and used regularly in commerce. As such, we urge the Committee to narrow the items included in the definition.

We also strongly recommend that the definition of sensitive financial identity information exclude information that is otherwise available from public sources. It is impractical and unworkable to require businesses to be held liable when the data is publicly available (whether over the Internet or from government offices or libraries). From the consumer perspective, there is little benefit in being notified where the information is otherwise available from public sources. We note for the Committee that the vast majority of states (18) that have adopted laws have included exceptions for publicly available information.

SIIA commends the bill for taking steps to avoid unnecessary or frivolous litigation by vesting "exclusive" responsibility for enforcement with the agencies of functional jurisdiction. To avoid the very real risk of unnecessary litigation, we urge that the legislation recognize that private rights of action or class actions that are premised in whole or in part upon the defendant violating any provision of the bill are counterproductive and should be precluded.

HR 3997 utilizes the enforcement framework of the Fair Credit Reporting Act. As a consumer protection statute, SIIA supports full enforcement of the FCRA, and many of our members supported the amendments made in the last Congress by the Fair and Accurate Credit Transaction Act (FACTA).

As a means for establishing an enforceable national framework on data breaches and notifications, we believe the following should be considered by the Committee:

First, most SIIA members are already subject either to the FTC's enforcement authority under Section 5, which builds on the "Safeguards Rule" of the Gramm-Leach-Bliley Act, or in some limited cases, to the provisions of the GLBA. Through cases brought under Section 5, the FTC has found a variety of unfair and deceptive practices ranging from failure to implement appropriate information security programs[3] to deceptive security claims made by companies.[4]

---

[3] *BJ's Wholesale,* (FTC Docket No. 042 3160)(June 16, 2005).

[4] See *Petco Animal Supplies, Inc.* (FTC Docket No. C-4133) (Mar. 4, 2005); *MTS Inc., d/b/a TowerRecords/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.)

However, HR 3997 leaves companies that are already subject to Section 5 enforcement open to duplicative and even contradictory requirements.[5] As we read HR 3997, nothing in the bill addresses this potentially confusing enforcement situation.

Second, HR 3997 defines a "financial institution" as any company that maintains the social security numbers of its employees or maintains a taxpayer ID number of its customers. We are deeply concerned that this definition extends the concept of "financial institution" well beyond any that has been used to date, and potentially brings a wide range of companies under the FCRA in a manner that was not anticipated when the FCRA was enacted or updated.[6]

In addition, the definition of "consumer report" has been changed to include any report "bearing on a consumer's ...personal identifiers..." and therefore subject to the FCRA. While it remains unclear what "bearing on" implies, there is great concern that the practical effect of this change is to cause any business disseminating information that contains "personal identifiers" -- an undefined term in HR 3997 -- to potentially be regulated as a consumer reporting agency under the FCRA regardless of how commonplace those identifiers are. Those businesses could find their ability to sell common products using common "identifiers" -- such as alumni directories or "who's who" directories -- to be restricted to only those buyers with a permissible purpose under the FCRA, a change that would have a catastrophic effect on those businesses.

Third, we share the bill's goal of effectively preempting state laws by having a national framework supersede any state or local requirements. At the same time, we are cognizant that case law is emerging on the *scope* of federal prerogatives in this area, even where tightly written language on preemption has been incorporated, as appears to have been done in HR 3997.

For example, the Ninth Circuit in this area "generally presume[s] that Congress *has not intended* to preempt state law, starting 'with the assumption that the historic police powers of the States [are] not to be superseded by [federal legislation] unless that is the clear and manifest purpose of Congress.'"[7] In determining whether the specific preemption provisions of the FCRA supersede California Senate Bill 1 – which is directly targeted at financial information – the analysis of the federal courts in the 9th Circuit rests on whether the information "fall[s] within the scope of information governed by the FCRA" and whether the information is for a "FCRA authorized purpose."[8]

---

[5] HR 3997 includes provisions designed to avoid duplication with GLBA, and our more detailed comments to HR 3997, which we will submit after the hearing, includes suggestions to improve these particular provisions.

[6] At the same time, we note that a "financial institution" *as currently defined* is exempted from the requirements of HR 3997

[7] *ABA v. Lockyer*, Docket No. CV-04-00778-MCE (9th Circuit), decided June 20, 2005, citing *Cipollone v. Liggett Group, Inc.*, 505 516 (1992) (internal brackets, citation, and quotation marks omitted in original).

[8] ABA v. Lockyer, E.D.Calf., decided on remand from the 9th Circuit, October 6, 2005.

To date, no state enacting a data breach notification law (including those with safeguards provisions) has limited the scope of its law to the financial sector or to specifically regulated information. This is especially true of the first such state law enacted in California. SIIA looks forward to working with the Committee to achieve the shared goal of enacting a meaningful national framework that avoids courts having the last word on whether federal law preempts state laws in this area.

Mr. Chairman, to ensure that a coherent policy approach is achieved by Congress, we once again urge this Committee to continue its work on this bill and to work with other relevant Committees as the process unfolds. We appreciate the opportunity to appear before you today. I will be glad to take any questions that you might have.

Testimony

Of

Assistant Attorney General Julie Brill
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609-1001
Tel: 802-828-3658

Email: jbrill@atg.state.vt.us

before the

Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives

Hearing on H.R. 3997, the Financial Data Protection Act

November 9, 2005

Good morning, Chairman Bachus, Ranking Member Sanders, and distinguished members of the Subcommittee on Financial Institutions and Consumer Credit. Thank you for inviting me to speak with you today on the important issue of security breaches and protection of personal information. My name is Julie Brill, and I am an Assistant Attorney General for the State of Vermont. I have been working in the consumer protection arena in Vermont for 14 years, specializing in privacy and data security issues, among other things. In addition, I am chair of the National Association of Attorneys General Working Group on Privacy, and chair of the National Association of Attorneys General Working Group on Credit Reporting. In these capacities, I have worked with the National Association of Attorneys General on numerous national issues relating to privacy, security breaches and data security, including comments to Congress and various federal agencies. I testify this morning on behalf of the National Association of Attorneys General as well as Vermont Attorney General William H. Sorrell.

There have been reports of over 118 data leaks this year, which taken together have affected 57 million consumers in the United States.[1] The security breaches have exposed millions of consumers to potential identity theft, a serious and rapidly growing crime that now costs our nation over $50 billion per year. Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by theft of personal information. As a result of California's innovative state law, now adopted by 21 additional states, the public has become aware of these numerous

[1] See Choicepoint's 2005 Disclosures of US Data Incidents, available at http://www.privacyatchoicepoint.com/common/pdfs/Datadisclosures2005.pdf .

data leaks.[2] State security breach notification laws have provided consumers with vital information about unauthorized access to their personal information, so that the affected consumers can take precautions to ensure that they do not become victims of identity theft, or that any harm they experience as a victim of identity theft is minimized.

The National Association of Attorneys General is gratified that this Committee is considering legislation to create a federal security breach notification law modeled on state laws. The issue is of such importance that just two weeks ago, 48 State Attorneys General set forth their views on the appropriate contours of any federal law in a letter to the Congressional leadership.[3] The letter is attached to my written testimony and dated November 7, 2005, to reflect all signatories to date.

In their letter, the Attorneys General call on Congress to enact a strong federal security breach notification law that provides meaningful information about data leaks to consumers. If Congress is unable to enact a strong notice law, then the Attorneys General suggest that Congress leave the issue to the states, which have responded rapidly and strongly to the problems presented by security breaches.

The Attorneys General believe an effective federal security breach notification law would contain the following elements.

---

[2] The following states have enacted security breach notification laws: Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington.

[3] The original letter, dated October 27, 2005, was signed by the Attorneys General of Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Northern Mariana Islands, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming. The Attorney General of New Mexico joined the letter a few days after it was originally sent. The letter is now dated November 7, 2005.

- The federal law should broadly define "security breach" as unauthorized acquisition of or access to computerized, paper or other data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. There should be no additional requirement that the breach entail actual harm or a measure of risk of harm.
- In the event that Congress decides to consider the concept of harm in addition to the unauthorized acquisition of personal information before notice would be required, the "harm" element should be an exception, not a trigger, in order to make it plain that a notice must be given in the absence of sufficient information. Security breach notices should be provided to consumers ***unless there is no risk of harm or misuse of personal information*** resulting from the breach.
- The breached entity should be required to consult with law enforcement and receive an affirmative response that there is no risk of harm or misuse of personal information from the breach before the "harm" exception would apply.
- All entities, including financial institutions governed under the Gramm-Leach-Bliley, should be covered.
- There should be no "fraud monitoring" exception, especially with respect to compromised information relating to debit card, bank account and other non-credit card account information.

The Attorneys General believe that Congress should ensure that the federal security breach notification law can be enforced by the State Attorneys General in state or federal court. Federal regulators like the Federal Trade Commission require assistance from local law enforcement in many areas affecting consumers, including telemarketing, credit reporting, and general unfair and deceptive practices. State Attorneys General are currently involved in investigating security breaches, and Congress should ensure that the Attorneys General continue to protect consumers in this important area.

Lastly, but most importantly, the Attorneys General urge Congress not to preempt state security breach notification laws. In the event that Congress considers preemption of state laws in this area, such preemption should be narrowly tailored so that only state laws that are "inconsistent" with the federal law are affected, and then "only to the extent of the inconsistency". The federal law may govern the timing, manner and content of security breach notification laws, but should not interfere with state laws addressing notices to be provided by entities not covered by the federal law or the consequences of security breaches.

Thank you for giving me this opportunity to testify on this important subject. I will be happy to answer questions.

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
750 FIRST STREET NE SUITE 1100
WASHINGTON, D.C. 20002
(202) 326-6018
(202) 408-6998
http://www.naag.org

LYNNE M. ROSS
Executive Director

PRESIDENT
STEPHEN CARTER
Attorney General of Indiana

PRESIDENT-ELECT
THURBERT BAKER
Attorney General of Georgia

VICE PRESIDENT
LAWRENCE WASDEN
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

November 7, 2005

Honorable Bill Frist
Senate Majority Leader
509 Senate Hart Office Building
Washington, D.C. 20510-4205

Honorable Harry M. Reid
Senate Minority Leader
528 Senate Hart Office Building
Washington, D.C. 20510-3903

Honorable J. Dennis Hastert
Speaker of the House
235 Cannon House Office Building
Washington, D.C. 20515-1314

Honorable Nancy Pelosi
House Minority Leader
2371 Rayburn House Office Building
Washington, D.C. 20515-0508

Dear Congressional Leaders:

We, the undersigned Attorneys General, applaud the efforts of the various committees in Congress which are considering enactment of a national security breach notification and security freeze law. Over the past year, the public has become aware of numerous incidences of security breaches, exposing millions of consumers to harm, including potential identity theft, a serious and rapidly growing crime that now costs our nation over $50 billion per year. The issues under consideration by you and your members could provide critical assistance to identity theft victims in our states and throughout the nation.

To assist your efforts, we offer the following comments, representing our views on certain critical issues relating to your consideration of security breach notification and

security freeze legislation.

1. **Enact a strong security breach notification law**

We call on Congress to enact a national security breach notification law that will provide meaningful information to consumers. If Congress is not able to enact a strong notice law, it should leave the issue to state law, which is responding strongly. Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by theft of personal information. The Federal Trade Commission (FTC) reports that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly. For example, when the misuse was discovered within five months of its onset, the value of the damage was less than $5,000 in 82% of the cases. When victims did not discover the misuse for six months or more, the value of the damage was $5,000 or more in 44% of the cases. In addition, new accounts were opened in fewer than 10% of the cases when it took victims less than a month to discover that their information was being misused, while new accounts were opened in 45% of cases when six months or more elapsed before the misuse was discovered.

The public has become aware of the numerous incidences of security breaches over the past year as a result of California's security breach notification laws, which went into effect on July 1, 2003. These laws require businesses and California public institutions to notify the public about any breach of the security of their computer information system where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The public has become so concerned about security breaches and their potential

role in the increased incidence of identity theft that 21 additional states have enacted security breach notification laws over the past year: Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington.

We urge your committee to enact a meaningful federal security breach notification provision that is at least as protective of consumers as California law. A meaningful federal security breach notification law would, in our view, broadly define what constitutes a security breach and the notice requirements in order to give consumers a greater level of protection. For example, "security breach" should be broadly defined as "unauthorized acquisition of or access to computerized or other data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." We also believe that the standard for notification should be tied to whether personal information, whether in electronic or paper form, was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud. It is certain, however, that creating an additional trigger requirement relating to proof of risk will result in fewer notices than consumers now receive under many state laws. We note that the majority of states that have enacted security breach notification laws – California, Georgia, Illinois, Indiana,

Maine, Minnesota, Nevada, New York, North Dakota, Ohio, Rhode Island, Tennessee, and Texas – do not require any additional trigger requirement before notice about a breach is required to be given to affected consumers.

In the event that Congress decides to consider the concept of harm in addition to the unauthorized acquisition of personal information in the context of security breach notification, we urge Congress to cast this element as an exception, not a trigger, in order to make it plain that notice must be given in the absence of sufficient information. Such an exception could contain the following provisions: (1) security breach notices must be provided to consumers unless there is "no risk of harm or misuse of personal information" – not "no risk of identity theft" – resulting from the breach; (2) security breach notices must be provided to consumers in the event that it cannot be determined whether or not there will be a risk of harm or misuse of personal information; (3) the breached entity should be required to consult with law enforcement and receive an affirmative written response with respect to the determination that there is no risk of harm resulting from the breach; and (4) any determination by law enforcement that there is "no risk of harm or misuse of personal information" should be made in writing and filed with both the FTC and with the State Attorney General from the state in which the breach occurred.

In addition to an acquisition-based notification standard, we believe that an effective federal security breach notification law should have the following additional provisions:

- Coverage of all entities, including financial institutions governed by the Gramm-Leach-Bliley Act. Financial institutions, which may hold very sensitive data

about consumers, should not be subject to a lesser standard for giving notice under their regulatory guidelines than other entities are held to by statute.

- Inclusion of the following as "personal information" that, if acquired or accessed by an unauthorized person, would trigger notification: an individual's first name or first initial and last name, or the name of a business, in combination with any one or more of the following data elements, when either the name or the data element is not encrypted:
    - Social Security number.
    - Driver's license number or government-issued identification number.
    - Account number, credit or debit card number, alone or in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    - A unique electronic identification number, email address, or routing code alone or in combination with any required security code, access code, or password.
    - Unique biometric data such as fingerprint, voice print, a retina or iris image, or other unique physical representation.
    - Home address or telephone number.
    - Mother's maiden name.
    - Month and year of birth.
    - Such other information as the FTC may add by regulation.
- Notification provisions that would, at a minimum, provide the following notices to consumers: individual notice by mail or by email if the consumer has

consented to email in a manner consistent with the requirements of the Electronic Signatures in Global and National Commerce Act; substitute notice, if permitted at all, could be an option only when more than 500,000 consumers are affected and should require publication on a website and in major statewide or national news media.

- No "fraud monitoring" exemptions, especially when the compromised information relates to a debit card, bank account, or other non-credit account.

2. Enact a strong federal security freeze law.

We also call on Congress to enact a strong federal security freeze law. The 2003 amendments to the federal Fair Credit Reporting Act gave consumers the right to place a "fraud alert" on their credit reports for at least 90 days, with extended alerts lasting for up to seven years in cases where identity theft occurs. Several states have enacted stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches. Five states – California, Louisiana, Texas, Vermont, and Washington – already allow consumers to place a "security freeze" on their credit report. A security freeze allows a consumer to control who will receive a copy of his or her credit report, thus making it nearly impossible for criminals to use stolen information to open an account in the consumer's name. Security freeze provisions will become effective in the next several months in the following additional seven states: Colorado, Connecticut, Illinois, Maine, Nevada, New Jersey, and North Carolina.

We believe that security freeze laws that give all consumers the right to use a freeze as a prevention tool are one of the most effective tools available to stop the harm that can result from data heists. If Congress is inclined to create a federal security freeze

law, we urge Congress to make such a law meaningful by modeling it on the best provisions in comparable state laws, including:

- Creating a security freeze that is available to all consumers at no fee or a low-capped fee.
- Banning fees for victims of identity theft who have a police report or FTC affidavit, seniors, veterans, and persons who receive a notice of security breach.
- Allowing consumers who choose to implement a freeze to also have the ability to selectively or temporarily lift the freeze, again at no charge to victims of identity theft, seniors, veterans, and persons who receive a notice of security breach, and to other consumers at a modest, capped fee.
- Ensuring that the security freeze provisions apply to all entities who may examine a credit file in connection with new accounts, including accounts for goods and services, such as cell phones, utilities, rental agreements, and the like.
- Allowing consumers who choose to implement a freeze with all three major national consumer reporting agencies to be able to do so by contacting one of them, rather than all three individually.

3. Allow the State Attorneys General to enforce the new federal security breach notification and security freeze laws in state or federal court.

We further call on Congress to ensure that State Attorneys General can enforce any new federal security breach notification and security freeze laws. The FTC continues to do a commendable job in enforcing its current laws, including the FTC Act and the

Gramm-Leach-Bliley Act, against entities that have not employed sufficient protections to safeguard consumers' personal information. However, consumers would suffer if Congress were to make the FTC the sole enforcer of new laws requiring security breach notification and security freezes. Indeed, State Attorneys General are currently involved in investigating security breaches and enforcing available state standards relating to use of adequate procedures and processes to protect consumers' personal information. Congress should ensure that State Attorneys General continue to play their important role in protecting consumers from practices that could lead to identity theft.

4. Do not preempt the power of states to enact and enforce state security breach notification and security freeze laws.

We urge Congress to not preempt the states in these two important consumer protection areas, or indeed in other areas. Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.

In the event that Congress determines that it will consider preemption of the states in these areas, we urge Congress at a minimum to narrowly tailor preemption so that only those states laws that are "inconsistent" with the federal laws would be preempted, and then "only to the extent of the inconsistency." This is important because Congress may enact a security breach notification law or a security freeze law that does not cover all entities, and the states should be allowed to enact laws that cover those additional entities. While we oppose preemption in general, it is particularly important that if Congress does

adopt some degree of preemption, that preemption be limited to the timing, manner, and content of notices of security breach, and not interfere with other state laws addressing the subject of, or consequences of, a security breach.

Thank you for considering our recommendations. We look forward to working with you on this important legislation in the coming weeks and months.

Sincerely,

David W. Márquez
Attorney General of Alaska

Terry Goddard
Attorney General of Arizona

Mike Beebe
Attorney General of Arkansas

Bill Lockyer
Attorney General of California

John Suthers
Attorney General of Colorado

Richard Blumenthal
Attorney General of Connecticut

M. Jane Brady
Attorney General of Delaware

Robert J. Spagnoletti
Attorney General of District of Columbia

Thurbert E. Baker
Attorney General of Georgia

Mark J. Bennett
Attorney General of Hawaii

Stephen H. Levins, Executive Director
Hawaii Ofc. Consumer Protection

Lawrence G. Wasden
Attorney General of Idaho

Lisa Madigan
Attorney General of Illinois

Gregory D. Stumbo
Attorney General of Kentucky

G. Steven Rowe
Attorney General of Maine

Tom Reilly
Attorney General of Massachusetts

Mike Hatch
Attorney General of Minnesota

Jay Nixon
Attorney General of Missouri

Jon Bruning
Attorney General of Nebraska

Kelly Ayotte
Attorney General of New Hampshire

Patricia A. Madrid
Attorney General of New Mexico

Tom Miller
Attorney General of Iowa

Charles Foti
Attorney General of Louisiana

J. Joseph Curran, Jr.
Attorney General of Maryland

Mike Cox
Attorney General of Michigan

Jim Hood
Attorney General of Mississippi

Mike McGrath
Attorney General of Montana

Brian Sandoval
Attorney General of Nevada

Peter C. Harvey
Attorney General of New Jersey

Eliot Spitzer
Attorney General of New York

Roy Cooper
Attorney General of North Carolina

Pamela Brown
Attorney General of Northern
Mariana Islands

W.A. Drew Edmondson
Attorney General of Oklahoma

Tom Corbett
Attorney General of Pennsylvania

Patrick Lynch
Attorney General of Rhode Island

Larry Long
Attorney General of South Dakota

Greg Abbot
Attorney General of Texas

William H. Sorrell
Attorney General of Vermont

Wayne Stenehjem
Attorney General of North Dakota

Jim Petro
Attorney General of Ohio

Hardy Myers
Attorney General of Oregon

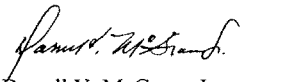
Roberto J. Sanchez-Ramos
Attorney General of Puerto Rico

Henry McMaster
Attorney General of South Carolina

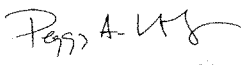
Paul G. Summers
Attorney General of Tennessee

Mark Shurtleff
Attorney General of Utah

Rob McKenna
Attorney General of Washington



Darrell V. McGraw, Jr.
Attorney General of West Virginia



Peggy A. Lautenschlager
Attorney General of Wisconsin

Patrick J. Crank
Attorney General of Wyoming

cc: Chairman Shelby & Ranking Member Sarbanes
Senate Committee on Banking, Housing, and Urban Affairs

Chairman Stevens & Ranking Member Inouye
Senate Committee on Commerce, Science, & Transportation

Chairman Specter & Ranking Member Leahy
Senate Committee on the Judiciary

Chairman Barton & Ranking Member Dingell
House Committee on Energy & Commerce

Chairman Oxley & Ranking Member Frank
House Committee on Financial Services

Chairman Sensenbrenner & Ranking Member Conyers
House Committee on the Judiciary

1. Of the states listed, Hawaii is also represented by its Office of Consumer Protection, an agency which is not a part of the state Attorney General's Office, but which is statutorily authorized to represent the State of Hawaii in consumer protection actions. For the sake of simplicity, the entire group will be referred to as the "Attorneys General," and such designation as it pertains to Hawaii, refers to the Attorney General and Executive Director of the State of Hawaii Office of Consumer Protection.

Testimony of
America's Community Bankers
on

"H.R. 3997, the Financial Data Protection Act of 2005"

before the

Subcommittee on Financial Institutions
and Consumer Credit

of the

Financial Services Committee

of the

United States House of Representatives

on
November 9, 2005

Josie Callari
Senior Vice President
Astoria Federal Savings
Lake Success, NY
and
Chairman
ACB Electronic Banking and Payment Systems Committee

Chairman Bachus, Ranking Member Sanders, and members of the committee. My name is Josie Callari, and I am testifying today on behalf of America's Community Bankers.[1] I am Senior Vice President of Astoria Federal Savings, headquartered in Lake Success, New York. Astoria Federal Savings is a full service financial institution providing retail banking services to the New York City area, and home financing to 14 states. I have 30 years experience in the banking industry, ranging from my start in a retail branch to my current position as Director of Banking Operations at Astoria Federal Savings, with a staff in excess of 200. In addition to my duties at Astoria Federal Savings, I serve as Vice Chairman of ACB's Electronic Banking and Payments Committee.

ACB appreciates having the opportunity to testify before the Subcommittee on H.R. 3997, the Financial Data Protection Act. The issue of data security is critical for community banks. The number of high-profile data breaches that occurred this year brought to light possible vulnerabilities that have been created due to the Internet revolution. While banks have had the mandate to safeguard sensitive customer information for years, the growth of the Internet and electronic commerce has made compiling and selling sensitive personal information easier for a multitude of companies, creating a need for comprehensive data security legislation.

That is why ACB supports H.R. 3997, introduced by Congressmen LaTourette, Hooley, Castle, Pryce, and Moore. This legislation is a common sense approach to providing a meaningful solution. Identity theft and account fraud are real and growing crimes in the United States, and the expanding amount of consumer information that is collected and stored by businesses has the potential to feed the identity theft problem. This country needs legislation that addresses the problem, not the symptom. That means focusing on stopping the misuse of consumer information, and creating an incentive for companies to make securing customer data a priority. Mr. Chairman, ACB believes that H.R. 3997 achieves this goal in a way that protects consumers, helps to prevent the abuse of consumer information, and gives companies an incentive to do the right thing, while maintaining maximum flexibility for all types of businesses.

Review of H.R. 3997

Let me start discussing ACB's view on H.R. 3997 by giving a background of ACB's principles for all data security legislation. Earlier this year ACB's board of directors laid out its top priorities for any data security legislation that may be considered in Congress. These priorities included:

1) Creating a national standard
2) Exempting institutions subject to existing GLBA data security requirements
3) Maintaining functional regulation
4) Providing full reimbursement of costs by those responsible for security breaches

[1] America's Community Bankers is the member-driven national trade association representing community banks that pursue progressive, entrepreneurial and service-oriented strategies to benefit their customers and communities. To learn more about ACB, visit *www.AmericasCommunityBankers.com*.

ACB is pleased to see that H.R. 3997 addresses our top three priorities, and that it begins to deal with the difficult issue of reimbursement.

National Standard

Having a national standard is critical for any legislation addressing data security and consumer notices. Adding another layer of regulation to a rapidly growing patchwork of state and local laws hurts consumers, hurts the economy, and will not provide effective protection. Our nation's economy has evolved to the point where commerce and banking are nationwide activities. People can travel anywhere in our country at any time, and thanks to the Internet, conduct business throughout the nation from the comfort of their home. When it comes to the nation's payment systems, borders mean little. A Balkanized patchwork of state laws that provide protections that stop and start at state lines will not provide meaningful protection for consumers in a national marketplace. Over 40 million Americans move every year, and they expect to have the same protection of sensitive personal information in their new home as they did in their old. Having a uniform national standard for data security and breach notices will afford them that protection. Furthermore, consumer information should be protected equally regardless of the state where the transaction occurred. Consumers deserve uniform protection, and ACB believes that the Congress has an obligation to provide it.

Gramm-Leach-Bliley Exemption

Additionally, ACB believes that Congress should recognize that the Gramm-Leach-Bliley Act (GLBA) already requires financial services companies to have in place much of what is being considered in most data security legislation. Title V of GLBA requires financial services companies to implement data security safeguards, a customer response program, and a comprehensive privacy policy. This spring the banking regulators issued guidance extending Title V to require customer notices in case of a breach that puts consumers at risk. To layer a duplicative regulatory system on top of this robust framework would only increase costs for financial institutions, and ultimately their customers. Such a system is unnecessary and ultimately would be harmful.

In addition, ACB applauds the committee for requiring that regulators work to harmonize existing GLBA standards to the greatest extent possible with those that will be required for non-financial institutions. Consumers should not experience different protection for their sensitive information based on what type of company they do business with. However, I urge that the committee work to ensure that any new rules do not place unnecessary burdens on financial institutions, and recognizes that they do have some unique needs and requirements.

Functional Regulation

Likewise, financial institutions have an incredibly robust regulatory framework under which they operate. This is particularly true for depository institutions. The banking regulators regularly examine financial institutions to ensure safety and soundness and consumer protection. ACB applauds H.R. 3997 for embracing this existing framework by vesting enforcement with functional regulators. This will result in both a more efficient regulatory structure and more

uniform consumer protections. Some have contemplated a system where enforcement would be vested with various state entities, such as state Attorneys' General. This would lead to uneven enforcement, where enforcement might depend on arbitrary local considerations rather than a uniform, predictable approach to national enforcement. As a banker I have grave concerns about such a system because it could infringe upon the principles of the dual chartering system for financial institutions. As I said earlier, the protection of a person's sensitive personal information should not depend on where they live or where a particular company is located. This is unfair for consumers. We need uniform enforcement, and vesting enforcement with established agencies of national scope and responsibility achieves that goal in an efficient and reliable manner.

Other Important Provisions

I also would like to highlight some of the other parts of H.R. 3997 that ACB supports. One of the most difficult aspects of crafting legislation to prevent the misuse of consumer information is creating a trigger that will notify consumers when they are at risk for fraud or identity theft, but not inundate them with unnecessary notices that cause unnecessary concern and ultimately desensitize consumers. By using a standard of "reasonably likely" to cause harm, the legislation has struck a good balance between the need to notify and the objective of providing meaningful notices. Additionally, ACB applauds the committee for recognizing the difference between account fraud and identity theft. These two distinct problems have often become blurred as one in popular debate, but for consumers there is a distinct difference between the two risks. Transaction fraud poses minimal risk to consumers because they have no liability for fraudulent credit or debit card transactions, and regulations specify standards for speedy resolution. Transaction fraud generally creates only a temporary inconvenience. However, identity theft can be much more harmful for consumers, and they must take concrete steps to prevent identity theft as quickly as possible if they are at risk. The dual notices recognize these differences and provides consumers with the appropriate information to address the risk.

Finally, ACB supports efforts to ensure that banks have the ability to be part of an investigation into possible breaches. The requirement for joint investigations between companies and their third parties helps to ensure that community banks will not be left in the dark when an investigation is ongoing. Furthermore, requiring that contracts between companies and their third parties address who is responsible for sending notices is very important. Many community banks believe they should be the ones to send breach notices to their customers, regardless of who is responsible for the breach. Community banks are proud of the relationships they have with their customers, and generally would prefer be responsible for sending a breach notice, rather than what is likely to be an unknown company communicating with the bank's customers.

Potential Area of Concern with H.R. 3997

As I mentioned before, ACB supports H.R. 3997, and hopes to see the committee act quickly on it. However, there are two areas where ACB's members have concerns, and we look forward to working with the committee and the bill's sponsors to address these concerns. First and foremost, ACB believes that those who are responsible for a data breach must be responsible

for the costs of protecting consumers from risks arising from the breach. The committee has taken the first step towards this by requiring that the party responsible for the breach should bear the cost of sending notices. This is common sense, but notices are only a small part of the cost of protecting consumers. One of the biggest costs is that of reissuing credit and debit cards, and closing accounts placed at risk. ACB's members have estimated that the replacing cards can cost up to $15. In instances where a community bank has thousands of cards affected these costs can mount quickly, and the institution ends up bearing all of the costs itself. Community banks are doing this now because they are dedicated to protecting their customers, however, they should not have to bear those costs. Those responsible for the breach should bear them.

Finally, ACB's members have expressed concern that there is no limit on how long an investigation required under a bill can take. Our members support the structure requiring investigations, which allow companies a chance to assess the severity of a potential breach, and the risk it poses to consumers. This is a responsible approach and allows companies the flexibility they need to protect consumers. However, ACB's members are concerned that without guidance the investigations could take an excessively long time, leaving consumers at risk. We believe that it is not advisable to legislate hard deadlines for investigations because each one is unique and will require a different response. However, the bill should require that as part of the overall rulemakings, regulators should give guidance on the appropriate length of an investigation.

Conclusion

In conclusion, ACB supports H.R. 3997 and urges the committee to consider it soon so that consumers can enjoy the protections it would provide. ACB urges that H.R. 3997 be passed with constructive modifications such as those suggested, but without adding provisions that take the bill's focus away from securing consumer data, providing appropriate and timely notices, and creating the right incentive structure and enforcement mechanism to stop the misuse of consumer information. This bill is crafted to be workable and effective, but adding provisions unrelated to its core purpose could jeopardize its potential benefits. We look forward to working with you as the committee crafts legislation that best addresses the problems of data security breaches.

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

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

By
Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The House Committee On Financial Services
Subcommittee On Financial Institutions & Consumer Credit
November 9, 2005

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of *Privacy Times*, a Washington newsletter since 1981. For the past 25 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

I am the author of the book, "Credit Scores and Credit Reports: How The System Really Works, What You Can Do." (2nd Edition, Privacy Times 2005)

Don't Pass HR 3997

HR 3997 does not adequately advance protection for the security and privacy consumer data. In fact, it could weaken existing protections. Worse, its sweeping preemption of State law would interfere with, and in some cases

potentially prevent, States from continuing their vital role of responding to these fast-evolving problems with effective and well-targeted solutions. Therefore, we urge the subcommittee not to move this bill in its current form. No action would be preferable to HR 3997.

Privacy

In the United States and around the world, "Privacy" is defined broadly. As the U.S. Supreme Court has recognized, "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[1] If consumers' information is not adequately protected by the entities that maintain it, then consumers unreasonably lose control over their information. The same is true if consumers can not gain access to information about them, or are not allowed to correct errors that are later sold to third parties. The same is true if outsiders are able to use consumers' data for impermissible purposes. These are but a few of the subject addressed by long-standing principles of Fair Information Practices (FIPs), 1973 report of the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems[2], the 1977 report of the U.S. Privacy Protection Study Commission (PPSC)[3], and the 1980 principles set forth by the Organization of Economic Cooperation and Development (OECD)[4], which were signed by U.S. Government and some 24 other nations.

Accordingly, the subject matters of HR 3997 are inextricably linked to the fundamental privacy rights of Americans.

www.PrivacyTimes.com P.O. Box 302 Cabin John, MD 20818
(301) 229 7002 (301) 229 8011 [fax] evan@privacytimes.com

[1] U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989)
[2] PPSC Report, Pg. 15.
[3] The five FIP principles of the HEW task force were: (1) there must be no personal data recordkeeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
[4] (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Participation; (8) Accountability

Year of The Data Security Breach: Americans' Demand Protection Grows

The San Diego-based Privacy Rights Clearinghouse has counted 80 data breaches since February, involving the personal information of more than 50 million people. The unfortunate string of highly publicized data-security breaches justifiably has heightened Americans' concerns, as well as their demands for better privacy protections, as reflected by a series of recent opinion polls.

For example, a September 2005 CBS News and *The New York Times* showed that 89 percent were concerned about the theft of their Social Security number, credit card numbers and other identity numbers, while seven percent were "not too concerned," three percent were not "concerned at all," and one percent "did not know."

"At a time when views about so many national issues divide along party lines, this issue transcends partisanship or ideology," CBS News reported. "Democrats, Republicans, liberals and conservatives – all express disapproval of companies collecting personal information, are concerned about privacy rights and identity theft, and call for the government to do more to regulate such activity. In fact, 68% of conservatives (and 69% of liberals) would like to see the government do more to address personal privacy issues."

Moreover, 83% of respondents said that it was "mostly a bad thing" that companies collect their personal information, including what they buy, their credit histories, and income information.

A Few Good Items

Whenever possible, I prefer to emphasize the positive. HR 3997's proposed provision of free monitoring to victims of data-security breaches is an important step forward, though I think one-year would be a preferable term to six months. I also favor making notices distinctive, with "exclusive color and titling," thereby increasing the chances that a notice will be noticed, and not discarded as "junk mail."

Disappointing Start

However, given the mounting evidence of glaring privacy problems, and the growing demand among Americans for stronger safeguards, HR 3997 is a most disappointing "first pass" at the issues raised by "The Year of the Data Security Breach."

Because of its shortcomings, it would appear to do more weaken, rather than strengthen, Americans' right to privacy. If HR 3997 represents as far as the subcommittee can go, then I would urge the subcommittee to refrain from further action. I am confident that, like me, millions of Americans would like to see a strong bill that would substantially broader their rights to improve control over their personal information. However, one now has to wonder at this point if that is a realistic prospect.

Here are a few problems with HR 3997:

- It fails to expand important privacy rights, like extending FCRA-styled rights to information brokers, or creation of a right to freeze disclosure of one's own credit report

- It would appear to dramatically weaken California's original breach-notification standard, which has proven very effective in ensuring that individuals (including non-Californians) were notified that they might be at risk.

- It would appear to weaken the straightforward data security standards of Gramm-Leach-Bliley by overlaying vague and potentially confusing standards that allow for broad exceptions and "safe harbors."

- Worst of all, it would appear to broadly preempt State action in this area at a time when States consistently have responded to these fast-evolving problems with effective solutions. If interpreted in a draconian fashion, it would conceivably preempt some 12 State laws allowing consumers to "freeze" disclosure of their credit reports – without even mentioning the term "freeze" in the bill.

Chicken Little

These concerns are not without foundation. While leading companies like ING Direct and E-Loan support new privacy rights for consumers, other financial services companies do not favor stronger privacy. In opposing them, they are known to predict hardship, or otherwise dissemble. In 2001, for example, when North Dakota voters became the first Americans to have the chance to vote for a statewide ballot initiative on an opt-in financial privacy law, the financial industry spent over $150,000 in advertising money attempting to convince the voters that the measure would result in economic doom for North Dakota. But North Dakotans didn't buy it: The privacy initiative won 72% to 27%.

In California, when faced with a similar statewide ballot initiative, the financial services industry reached a compromise with State Sen. Jackie Speier and her colleagues, resulting in enactment of SB 1. The bill created an "opt-in" standard for selling of bank data to third parties, and an "opt-out" standard for affiliate sharing. The ballot initiative was withdrawn.

Spokesmen for major banks said they could live with the bill. Jon Ross, a Citigroup lobbyist, told *The American Banker* on August 25, 2003, "We were part of this and are pleased with the work done—it's a good fair result for everyone."

In an August 14, 2003 press release, the California Bankers Association (CBA), said, "We believe that, with the latest changes, this proposal qualifies as both reasonable and workable in many, but not all, aspects... We want to be clear that CBA would much prefer a national standard to a patchwork of state or local privacy laws."

However, the financial services industry was successful in litigating against affiliate sharing, as a federal court said these important State-based protections for consumer privacy were preempted by federal law.

It is also worth noting that the credit reporting industry generally opposed the FACT Act proposal to entitle Americans to one free credit report per year. Congress wisely disregarded this opposition. Moreover, it appears that the increased attention to credit reports and to identity theft has proven to be a marketing boon for the credit reporting agencies, which appear to be expanding the sale of high-priced credit-monitoring services. In other words, by doing what was right for Americans, Congress appeared to help the credit reporting industry.

Accordingly, industry protestations over stronger privacy rights should be viewed with skepticism.

HR 3997

Notice. The California notice requirement is straightforward and workable: a notice requirement where there has been an unauthorized acquisition of an individual's name along with a Social Security Number, a driver's license number, or an account number and corresponding access code.

But under HR 3997, it appears that notice would only have to be if the company decides that the information obtained "is reasonably likely to be misused in a manner causing substantial harm or inconvenience against consumers" to commit either "identity theft" or to "make fraudulent transactions on financial accounts."

As my colleague Ed Mierzwinski, of U.S. PIRG, testified recently, "The best way to convince companies to keep data secure in the first place is to require notices whenever they do not. The fact that the company doesn't yet know whether or how the information will be misused should not be enough to excuse notice. Companies that lose information should not get to decide whether consumers need to take further action to protect their privacy. Consumers should be warned. As to the industry's so-called "sky is falling" argument that consumers might face too many notices, we are unaware that the California law has resulted in any frivolous notices. Below we also describe ways to make the notices clear."

Defining Substantial Harm Or Inconvenience. The bill would define "substantial harm or inconvenience" as a material financial loss to or civil or criminal penalties imposed on the consumer, or the need for the consumer to expend significant time and effort to *correct erroneous information* relating to the consumer . . . but does not include other harm or inconvenience that is not substantial, including changing a financial account number or closing a financial account.

This is a cramped view of the kinds of harms or inconveniences that consumers experience following security breaches. Apart from direct financial loss or correcting erroneous data, victims of security breaches typically must endure other inconveniences, such as more closely monitoring their monthly statements, or ordering credit reports, regularly monitoring their credit and other time-consuming chores. Perhaps the greatest harm or inconvenience is enduring the uncertainty of whether your information has fallen into the hands of criminals. If the data includes Social Security number (SSN), then the uncertainty can last a lifetime. If it includes credit card numbers or other identifiers, such information can sometimes be "leveraged" into obtaining SSNs. Either way, the consumer is at the short end of the stick.

In its enforcement action against BJ's Wholesale Club, the Federal Trade Commission further articulated why inconvenience arising from inadequate security was damaging to consumers.

> After the fraud was discovered, banks cancelled and re-issued thousands of credit and debit cards, *and consumers experienced inconvenience, worry, and time loss dealing with the affected cards*. Since then, banks and credit unions have filed lawsuits against BJ's and pursued bank procedures seeking the return millions of dollars in fraudulent purchases and operating expenses. According to BJ's SEC filings, as of May 2005, the amount of outstanding claims was approximately $13 million.

> The FTC alleges that BJ's failure to secure customers' sensitive information *was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers* and not outweighed by offsetting benefits to consumers or competition. [Emphasis added][5]

I strongly urge the subcommittee to hear directly from victims of data security breaches in reconsidering its definition of these terms.

Weakening Data Safeguards Standards?

Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB) mandated that financial institutions develop and implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Subsequent guidelines require each institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.[6] The GLB data security standards are intended in part to ensure that individuals maintain reasonable control over their personal data, as the standards recognize that failing to secure such valuable information greatly heightens the possibility it will fall into the wrong hands, thereby spiraling further out of the control of the individual.

But HR 3997 would appear to weaken these standards by shifting the focus away from protecting the data to maintenance of "reasonable policies and procedures," or as the bill states, "affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information...that is reasonably likely to result in substantial harm or inconvenience."

Unfortunately, even in cases where consumers were harmed or inconvenienced by bad security or faulty privacy practices, some financial institutions, in seeking to avoid responsibility, have insisted that their procedures were reasonable.[7]

---

[5] In the Matter of BJ's Wholesale Club, Inc., FTC File No. 042 3160; Also see, "BJ'S Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards," FTC Press Release, June 16, 2005; http://www.ftc.gov/opa/2005/06/bjswholesale.htm

[6] "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information," Office of the Comptroller of the Currency, OCC 2001-35, Attachment A; http://www.occ.treas.gov/ftp/bulletin/2001-35a.pdf

[7] In one pending FCRA case in which the plaintiff sued after a credit card company repeatedly "verified" disputed information that was false, the designated expert for the credit card company argued that plaintiff's lawsuit "confuse[d] (1) the requirement that the furnisher ***report accurately the results*** of its investigation (of the disputed data) to the credit reporting agency with (2) the requirement that the furnisher ***report accurately the information*** investigated." The argument put bad form ahead of substance.

People First

When fashioning privacy legislation, it is vital that the priority be increasing Americans' control over their personal information. Proposals that tilt toward the prerogatives of large organizations that wish to traffic in individuals' data will not solve the problem and ultimately require that Congress revisit these issues in the near future.

In addition, if we are to have national privacy standards, they must reflect a high level of protection. If uniformity is a priority, then Congress must get out in front of issues and, working with the States, establish high levels of privacy protection through national law.

As a practical matter, this has proven difficult. For instance, when I appeared before a House Financial Services subcommittee in April 2003, when the California breach notification was the only State law of its kind, I recommended that Congress adopt it as a national standard.[8] In hindsight, it might have been easier for Congress to do so at that time.

Instead, however, the States have continued to take the lead in protecting consumer privacy. I believe that at least 20 States have security-breach notice laws, and some 10 States have credit freeze laws. These laws are clearly having a national impact, benefiting millions of Americans – even where no State law exists.

Thus, if Congress wants to act in these or other areas of privacy, it is essential that it enact a strong federal measure.

Unfortunately, HR 3997 fails to accomplish this. Instead, it appears it would weaken standards and possibly make it easier for some large organizations to avoid their responsibility to protect the privacy of consumers' highly sensitive financial data.

Data Security Concerns Persist

In the October 25 issue of *Privacy Times*, we ran a story based on a former employee's allegations that data security was neglected at NOVA Information Systems, the nation's third largest credit card processor, much as it was at CardSystems Solution, which was hit by a breach and was the topic of a subcommittee hearing this July. As the story notes, NOVA vehemently denied the

[8] Fighting Fraud: Improving Information Security," House Financial Services Subcommittee on Financial Institutions & Consumer Credit, and Oversight, April 3, 2003; http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=202

charges and insisted it was and will continue to be compliant with Visa security standards. At this point, it is basically a "She said, it said" story. (Attached)

What struck me, however, was that it did not seem that any outside entity representing the public's interest would more closely examine NOVA to determine if *any* of the detailed allegations were valid. NOVA processes records on millions of consumers. I urge the subcommittee to look into this to determine if these allegations warrant Congressional oversight or examination by federal or State regulators.

In October, it appeared that a Trans Unions, a major credit reporting agency, suffered significant data breaches. A Midwestern bank was hit in the Spring, but it received little publicity.

Conclusions & Recommendations

If the subcommittee is unable to report out legislation that establishes high levels of protection for consumer privacy, then I see no justifiable reason for moving a bill. The State laws already are having a national impact. In privacy, once the bar is set high, there is a "race to the top." Any federal law that would lower the bar would be counterproductive. Preempting States from continuing their exemplary work would be potentially disastrous.

Here are some of my preliminary recommendations from my April 2003 testimony:

Expand & Improve Consumer Access to Their Own Financial Data. The FCRA already gives consumers the right to see their credit report and caps how much CRAs can charge. This approach needs to be upgraded to the electronic age and expanded to the entire realm of financial data, especially since large financial institutions are maintaining their profiles on customers, perhaps beyond the reach of the FCRA. In the meantime, Congress could pass a Resolution or Sense of the Congress that as a matter of principle and fundamental fairness, Americans should have a right to see and correct information about themselves. In light of ChoicePoint and Lexis Nexis, these rights should extend to information brokers as well.

Impose A General Duty To Notify Consumers After Data Leakages. The new California law provides a model starting point.

State Attorney General Enforcement. The State AGs consistently have brought important enforcement actions in a number of areas to ensure consumers' privacy rights. Failure to include State AG enforcement would leave a glaring hole and prove to be a major mistake.

Curtail The Use of SSNs as a personal identifier. Rep. Clay Shaw and others have introduced legislative proposals to this effect.

Create An Independent Privacy Office Most people don't realize that Sen. Sam Ervin originally proposed such an office along with the Privacy Act. Now, every advanced nation has one except the United States.

Create A Private Right Action So People Can Enforce Their Own Rights. Privacy affects virtually all 200 million adult Americans. In this electronic age, they must have rights, and those rights must be enforceable. You will never be able to build a bureaucracy big enough to adequately enforce Americans' right to privacy, nor should you want to. Thus, the private right of action is essential.

I'd be happy to answer any questions.

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 25 Number 20 October 25, 2005

CAPITAL INSIGHTS: Telecommunications firms, nonprofit organizations and educators are asking the U.S. Court of Appeals in Washington to overturn rules that would extend federal surveillance capability to the Internet. Authored by the Federal Communications Commission, the rules would extend the mandates of the Communications Assistance for Law Enforcement Act (CALEA). The 1994 law required telephone companies to rewire their networks and switches to make them "wiretap-friendly" to law enforcers. "The FCC simply does not have the statutory authority to extend the 1994 law for the telephone system to the 21st century Internet," said Marc Rotenberg, director of the Electronic Privacy Information Center. . . . Sen. Maria Cantwell (D-WA) has introduced a bill in the Senate Judiciary Committee that asks the Justice Department to investigate a link between ID theft and Methamphetamine use. "The meth epidemic is creating a wave of identity theft," she says. Meth addicts – already adept at stealing personal information from mailboxes to finance drug habits – now are hacking PCs to steal information, Bob Gauthier, a detective in the Edmonton, Alberta, Police Service's meth project team, told USA Today.

MAJOR STORIES IN THIS ISSUE

Ex-Employee Alleges Lax Security At Card Processor . . 1

U.S. Banking Agencies Back Online Authentication 4

FBI Violating Spy Curbs, According To EPIC Docs, . . . 4

Judge Strikes Down Georgia Voter Identification Law 6

Survey: Americans Want Both E-Health Data & Privacy . . . 7

Google Revises Policy After Reporter 'Googles' CEO . . . 7

FOIA Ct. Roundup: Scolding Aside, Customs Withholds . . 9

In Brief: College Aid Seen As Target Of ID Thieves 10

NOVA, U.S. BANCORP DENY CHARGES OF FORMER DATABASE ADMINISTRATOR

A former employee of NOVA Information Systems, the nation's third largest credit card processor, has charged that the company has neglected rudimentary data security safeguards, leaving vulnerable more than one billion credit card numbers and millions of business owners' Social Security numbers. In response to *Privacy Times* inquiries, the company denied the charges

Privacy Times Copyright © 2005

and expressed confidence that a Labor Dept. administrative law judge would dismiss her whistleblower-retaliation complaint.

Nell Walton, a database administrator (DBA) who took disability leave from her NOVA job in March, said that throughout 2004 and until her departure, she tried repeatedly to convince the company to bolster security for its mammoth computer systems so they would comply with Gramm-Leach-Bliley (GLB) rules, as well as audit standards of Visa Intl., the credit card association. (NOVA disagreed, insisting it was compliant with both GLB and Visa standards.)

However, the company disregarded her concerns and retaliated by increasing her workload, assigning menial tasks and with verbal harassment, she charged. Walton said the mounting stress forced her departure.

Walton's charges were listed in a July 2005 complaint to the Labor Dept.'s Occupational Safety and Health Administration (OSHA). It essentially alleged that she was retaliated against in violation of Section 806 of the Sarbanes-Oxley Act, the corporate governance law, for being a whistleblower. According to her complaint, the retaliation began shortly after a June 2004 meeting with Executive Vice President Erik Toivonen in which she outlined her concerns about data-security inadequacies. NOVA, which services more that 650,000 small and mid-sized merchants and banks, is owned by U.S. Bancorp, a publicly traded company. Walton's complaint seeks reinstatement and $1 million in damages.

This summer, an OSHA regional office dismissed her complaint, finding that Sarbanes-Oxley offered her no relief. Walton has appealed the dismissal to a Labor Dept. administrative law judge. She is represented by Thad Guyer, a private attorney who formerly worked for the Government Accountability Project (GAP), which specialized in whistleblower cases.

"The allegations are not true; they do not accurately reflect what her job duties were or the reaction of her supervisors," said Eric Savage, an attorney with the Newark, N.J. office of Littler Mendelson, representing NOVA. "The original decision to dismiss the complaint was correct and at the end of the day, we think the administrative law judge will come to the same conclusion."

Frank Erjavec, one of Walton's supervisors who was named in her complaint, flatly disputed her charges. "I don't think her charges are valid at all. We are VISA- and MasterCard-compliant. We are audited all the time. If you want to be in business with Visa and MasterCard, you have to take security seriously. We are constantly working on security issues," Erjavec told *Privacy Times*.

The largest potential security breach this year – 40 million credit card accounts – involved CardSystems Solutions, an Arizona-based credit card processing company. The highly publicized case prompted a Congressional hearing (see *Privacy Times*, Vol. 25 No.12, June 22, 2005). At one point, the transgressions prompted Visa to cancel the company's contractual right to process credit cards. (After passing subsequent audits, the company announced Oct. 15 it was acquired by "Pay By Touch," a payments technology firm.)

CardSystems was found to have improperly kept credit card data, and well beyond the contractual time limit. Walton accused NOVA of doing the same thing. The company denied this.

Walton said NOVA's security woes were the result of a combination of inadequate management attention, and staff training and resources, and outdated equipment. She said that several databases were vulnerable, including one housing more than 1.5 billion credit card numbers or authorizations, and another containing 650,000 to 1 million merchant records that included an owner's SSN, date of birth, home address, bank account and routing numbers. Walton also expressed concern about NOVA systems used by merchants to support e-commerce transactions, including "shopping carts."

Walton's complaint argued that Sarbanes-Oxley "requires publicly traded corporations to implement computerized safeguards or controls, both preventative and detective, against internal or external tampering, and against adulteration or negligence in the maintenance of its computer systems that create financial and operational records."

"[Walton] persisted in voicing and seeking resolution to concerns pertaining to [NOVA's] failure to comply ... [She] attempted to motivate compliance by disclosing these failures to corporate managers and was about to make said disclosures to external auditors. In retaliation for raising those concerns, [NOVA] subjected [Walton] to a continuing hostile and discriminatory work environment," the complaint alleged.

One oversight mechanism for NOVA's systems was the Visa audit process known as Customer Information Security Program (CISP). Walton praised the CISP standards, stating that compliance with them would greatly enhance security and help ensure compliance with other standards like GLB.

Walton's complaint stated that her concern over security heightened in early 2004 when NOVA assigned her to a CISP-compliance project with a Sept. 30, 2004 deadline.

"As the September 2004 completion date approached, [Walton's] security concerns led her to begin researching requirements for 'CISP' compliance," her complaint stated. "On November 2, 2004, Norman and Erjavec were found to have effected an unapproved database change, that is, one outside of the procedures and approvals prescribed in the Change Control Process."

Visa's "List of Compliant Service Providers" shows that NOVA was validated on Nov. 30, 2004. V.P. Erik Toivonen said NOVA was on target to pass the PCI Security audit next month. (Go to www.visa.com/CISP, then find on the left side the button for "Service Providers," and click; then find on the right side the "List of CISP-compliant service providers.")

Visa does not conduct audits. Instead, it has qualified about 20 companies to perform what it calls "onsite PCI Data Security Assessments for Level 1 Merchants and Levels 1 and 2 Service Providers and complete the Report on Compliance according to the PCI Security Audit Procedures and Reporting document." (Follow the link instructions above but instead of "List of CISP-compliant service providers," click on "Qualified Data Security Company List")

Toivonen said that Verisign conducted the Visa/CISP audits of NOVA in recent years. Steve Dale, a U.S. Bancorp spokesperson, along with attorney Eric Savage, said it was doubtful

that NOVA would provide *Privacy Times* with audit reports. Toivonen said that NOVA is subject to GLB, and has passed annual audits conducted by examiners from the Federal Reserve Board and the Office of the Comptroller of the Currency.

Citing OSHA's dismissal of Walton's charges and its Visa-compliant status, Dale said there was no merit to her allegations. "NOVA is and has been committed to protecting cardholder information in its internal and third party environments," he said.

A Federal Reserve spokesman said the board has jurisdiction over "holding companies" that own financial institutions. An OCC spokesman said he believed his agency also would have jurisdiction. Both spokesmen declined specific comment on the Walton case.

U.S. BANKING AGENCIES BACK TOUGHER ONLINE SECURITY

A federal panel composed of major U.S. banking agencies has issued new guidelines aimed at overhauling security in Internet-based banking and financial services, mandating stronger customer authentication requirements by next year.

Citing the growing threat posed by "phishing," identity theft, and other forms of online fraud, the U.S. Federal Financial Institutions Examination Council (FFIEC) said authentication of a customer via simple password and ID alone was "inadequate for high-risk transactions involving access to customer information or the movement of funds to other partners."

The council, which has broad regulatory powers over the banking sector, updated its guidance from 2001. The FFIEC is composed of member agencies that include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the

YES I Want To Subscribe & Save 10% Off The $340 Annual Rate

_____ $310 Per Year (23 Issues)
_____ $595 2-Year (46 issues)

_____
Credit Card No. (Visa, MC or Amex)

_____ Expiration Date

(Or you can pay by Check or Purchase Order)

Name _____
Org. _____
Address _____
City/ST/ZIP _____

Phone No. _____

Privacy Times
P.O. Box 302
Cabin John, MD 20818
(301) 229-7002 [Ph] (301) 229-8011 [Fax]

evan@privacytimes.com — www.privacytimes.com

TESTIMONY OF

OLIVER I. IRELAND

ON BEHALF OF THE

FINANCIAL SERVICES COORDINATING COUNCIL

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

ON

H.R. 3997

THE "FINANCIAL DATA PROTECTION ACT OF 2005"

November 9, 2005

Mr. Chairman and Members of the Subcommittee, my name is Oliver I. Ireland. I am a partner in the law firm of Morrison & Foerster LLP, practicing in the firm's Washington, D.C. office. I am here today on behalf of the Financial Services Coordinating Council, which consists of the American Bankers Association, the American Council of Life Insurers, the American Insurance Association and the Securities Industry Association. Together these associations represent a broad spectrum of financial services providers, including banks, insurance companies and securities firms. Our members have a strong interest in protecting our customers from identity theft and account fraud.

In general terms, identity theft occurs when a criminal uses personal identifying information relating to another person (generally, a name, address and Social Security number ("SSN")) to open a new account in that person's name. Identity theft can range from using a person's personal identifying information to obtain a cell phone, lease an apartment, open a credit card account, or obtain a mortgage loan or even a driver's license. In addition, in some cases, information relating to a person's financial account cannot be used to commit identity theft, but instead the information can be used to commit account fraud, that is, to initiate unauthorized charges to a person's financial account.

The issues of identity theft and account fraud, and related concerns about data security, are of paramount importance to financial institutions and the customers that we serve. Identity theft and account fraud can harm both consumers and financial institutions, and represent a challenge to law enforcement. A major priority of the financial services industry is preventing identity theft and account fraud before they

occur, and resolving those unfortunate cases that do occur. Both consumers and financial institutions benefit from a financial system that protects sensitive information relating to consumers, while remaining efficient, reliable, and convenient.

I would like to emphasize three key points:

I. Financial Institutions Are Already Regulated.

Unlike many other industries that maintain or process sensitive information relating to consumers, financial institutions and their customer information security programs are already subject to regulatory requirements. Further, financial institutions have a vested interest in protecting sensitive information relating to their customers, and work aggressively to do so.

II. A Uniform Approach Will Promote Information Security.

In today's world of nationwide financial markets, identity theft and account fraud do not recognize state boundaries. A consumer victim of identity theft may reside in one state, the identity thief may reside in another state, the financial institution victim of identity theft may be in a third state and the information that enabled the identity thief to perpetrate the crime may have been obtained in a fourth state. In this context, consumers will be most efficiently and effectively served by a uniform national standard applicable across financial services holding companies and to all entities that handle sensitive consumer information.

III. Security Breach Notification Requirements Should be Risk-Based.

Any security breach notification requirement should focus on those situations where a security breach creates a substantial risk of identity theft or account fraud. The alternative would result in over-notification of consumers. Over-notification about breaches of information security likely will needlessly alarm or desensitize consumers. Over-notification may lead consumers to ignore the very notices that explain the action they need to take to protect themselves from identity theft or account fraud or lead them to take unnecessary action in situations where the likelihood of identity theft or fraud may not exist. Notification should focus on situations that may lead to substantial harm to the consumer.

FINANCIAL INSTITUTIONS ARE ALREADY REGULATED

Among those that handle and process sensitive consumer information, financial institutions are among the most highly regulated and closely supervised. Title V of the Gramm-Leach-Bliley Act ("GLBA"), and associated rulemakings and guidance, require financial institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized accesses or uses and, in the case of banking institutions, to notify customers when there is a breach of security with respect to sensitive information relating to those customers.

Financial institutions must obtain and maintain sensitive personal information in order to serve their existing and prospective customers. Financial institutions have a strong, independent interest in protecting customer information and in having that information protected by third parties. Financial institutions that fail to earn and to

maintain the trust of their customers will lose those customers. Financial institutions have long recognized the importance of maintaining and protecting both the confidentiality and the security of this information and ensuring that it is not compromised.

In the competitive market for financial services, consumers tend to hold their financial institutions accountable for any problems that financial institutions experience with their account or information, regardless of the actual source of the problem. For example, if account fraud is committed as a result of a breach of security at a data processor working for a retailer—an entity that the account-holding financial institution does not control—the customer is likely to first seek a resolution through his or her financial institution. Therefore, information security is critical in order for financial institutions to maintain customer relations.

Financial institutions also are victims of identity theft, just as consumers are. For example, because banks do not impose the losses for fraudulent accounts on consumers and because financial institutions do not impose the losses associated with fraudulent transactions made on existing accounts on their customers, financial institutions incur significant costs from identity theft and account fraud. When a breach of information security occurs at a financial institution, the financial institution typically incurs costs in responding to that breach. Accordingly, financial institutions aggressively protect sensitive information relating to their customers.

Existing Data Security and Security Breach Notification Requirements

The federal banking agencies and the Securities and Exchange Commission have established regulations or guidance covering the security of customer information under section 501(b) of the GLBA. In addition, 34 states have adopted comprehensive regulations or statutes that establish standards for insurance companies with respect to safeguarding customer information. Under the customer information security guidance issued by the federal banking agencies, banks are required to notify their customers of breaches of security of sensitive information relating to those customers.

Going forward, any federal legislation should recognize the existing federal requirements that apply to financial institutions, and avoid subjecting financial institutions to duplicative and potentially inconsistent requirements. Further, federal legislation should recognize that financial institutions often operate in a holding company structure and also recognize the benefits to consumers and financial institutions from the "one-stop shopping" that the holding company structure facilitates. These benefits could be significantly impaired by the imposition of differing requirements on different types of financial institutions within a holding company. A financial services holding company should be able to apply existing and uniform federal requirements for data security and security breach notification to all institutions within the holding company.

In this regard, the state-based regulatory system for insurance companies reflected under the GLBA presents unique challenges. As noted above, 34 states have adopted customer information security requirements under section 501(b) of the GLBA. To date, only one state has adopted security breach notification requirements under that section.

Insurers, like other financial institutions, however, are subject to the non-uniform breach notification laws enacted by some 20 states. Given the critical need for uniformity and harmonization in data security and security breach notification requirements, particularly across financial services holding companies, insurers have no objection to new legislative requirements for data security as proposed in H.R. 3997 for insurers.

Insurers strongly support uniform national standards for the investigation and notice of security breaches and uniform enforcement of these standards. Accordingly, we support enforcement of insurers' compliance by the Department of the Treasury. If this is not possible, we support exclusive enforcement by the insurance authority of an insurer's state of domicile of both the statute and any implementing substantive regulations jointly promulgated by the relevant federal agencies.

A UNIFORM APPROACH WILL PROMOTE INFORMATION SECURITY

Uniform national standards applicable to all financial institutions are critical to providing meaningful and consistent protection for all consumers. All entities that handle sensitive consumer information—not just financial institutions—should be subject to similar information security standards. For example, retailers, data brokers and even employers collect sensitive consumer information, but many of these entities are not subject to data security and/or security breach notification requirements. Many of these entities, including data brokers, universities, hospitals, private businesses and even the Federal Deposit Insurance Corporation have been the victims of security breaches. Any entity that maintains sensitive consumer information should protect that information and should provide notice to consumers when a security breach has occurred with respect to

that information and the affected consumers need to take steps to protect themselves from identity theft or account fraud.

Uniformity Benefits Consumers

National uniformity is critical to preserving a fully functioning and efficient national marketplace. A score of state legislatures already have passed new data security laws. While these state laws have many similarities, they also have many differences. Millions of businesses—retailers, insurers, banks, employers, landlords and others—use consumer information to make important everyday decisions on the eligibility of consumers for credit, insurance, employment, or other needs. State laws that are inconsistent result in both higher costs and uneven consumer protection. The need to track these differences and factor them into a notification program may—particularly for small institutions—make it more difficult for institutions to send notice to consumers promptly. The complexity resulting from differing state requirements may mean that consumers will experience delays in receiving timely notices. Moreover, an individual state requirement or an individual state's failure to recognize a key provision can effectively nullify the policy choices made by other states. Under current state laws, the failure of one state to permit notices to be delayed for law enforcement purposes may frustrate law enforcement efforts in other states. A state with a breach notification requirement that is not risk-based can effectively override the laws of other states that provide for more targeted risk-based notices. Uniform guidelines applicable nationwide will ensure that consumers receive the same protections regardless of where they live.

SECURITY BREACH NOTIFICATION REQUIREMENTS SHOULD BE RISK-BASED

While it is important to protect all sensitive consumer information from unauthorized use, it is most critical to protect consumers from identity theft and account fraud. In order to avoid unnecessarily alarming and immunizing consumers to notices that information about them may have been compromised, security breach notification requirements, like the federal banking agencies guidance, should be limited to those cases where the consumer needs to act to protect himself or herself from substantial harm. Security breach notification requirements should provide clear triggers for notice and should be tailored to the circumstances and to the type of threat presented.

For example, a breach involving consumers' names and SSNs may or may not expose those consumers to the risk of identity theft depending on who obtains the information and the circumstances, particularly whether the information is encrypted or otherwise secured so that it is unreadable or unusable. Similarly, a breach involving account number information may pose no risk or cost to the consumer because of an antifraud program used by the consumer's financial institution or may require that the consumer simply follow established procedures to reverse erroneous charges to their accounts. In each case, the need for notification and the form that the notification should take will differ.

The federal banking agencies guidance under section 501(b) of the GLBA adopts a risk-based approach to security breach notification that encourages banking institutions to work with their federal regulators to address any suspected security breach. Upon the discovery of a breach of any size or scope, banking institutions are required to communicate the problem to their primary regulator and to begin devising a strategy to

best address that problem. Banking institutions are required to notify customers only where misuse of the information has occurred or is reasonably possible. This approach to security breach notification fosters close cooperation between banking institutions and their regulators in order to keep the focus where it belongs—protecting consumers. Although serious, a data security breach does not automatically, nor necessarily, result in identity theft or account fraud. Financial institutions store and transmit customer data in a variety of unique media forms that require highly-specialized and often proprietary technology to read, and may be subject to sophisticated encryption. Even if customer data finds its way into the wrong hands, the data often is not in a readable or useable form. Like the banking agencies guidance, federal legislation should recognize that the risks associated with each security breach will differ and, as a result, the appropriate response to each breach also will differ. As a result, federal legislation should adopt a risk-based approach to security breach notification, which takes into account the likelihood that the information has or will be used to harm consumers through identity theft or account fraud.

H.R. 3997

We commend the Subcommittee for its leadership role in developing this important legislation. We are pleased that H.R. 3997 clearly intends to provide a uniform national standard for data security and security breach notification and includes a number of other provisions that we believe are appropriate for federal security breach notification legislation. H.R. 3997, which would amend the federal Fair Credit Reporting Act ("FCRA"), applies broadly to virtually all entities that maintain sensitive information about consumers. Further, H.R. 3997 recognizes that financial institutions must comply

with existing GLBA requirements for data security and security breach notification, and attempts to ensure that these requirements are consistent across the financial holding company structure. H.R. 3997 provides for a risk-based notification scheme that does not require unnecessary notices to consumers. In providing for risk-based notices, H.R. 3997 recognizes that encryption and other means of securing consumer information can mitigate the likelihood of substantial harm and also recognizes the differences between breaches that involve information that can lead to identity theft and breaches that involve information that only can be used for account fraud. In addition, H.R. 3997 recognizes that appropriate risk-control systems can mitigate the risks of identity theft and account fraud and, therefore, any need for notification to consumers.

Finally, H.R. 3997 appropriately limits its focus to consumer information security and security breach notification and does not also address other issues, such as the ability of consumers to place "security freezes" on their credit reports and the regulation of the sale, display or use of SSNs.

With respect to security freezes, we believe that the FCRA fraud alert system adopted in the Fair and Accurate Credit Transactions Act of 2003 appropriately alerts creditors that certain consumers may be at risk for identity theft. It would be premature to discard this fraud system, which only recently became effective, in favor of a system of security freezes that could significantly disrupt the credit-granting process by preventing consumers from obtaining credit without going through time-consuming procedures to remove or temporarily lift security freezes.

With respect to potential limitations on the sale, display or use of SSNs, it is important to avoid unintended consequences. For example, disrupting the many

transactions that rely on these numbers, including the underwriting of and paying claims under insurance policies and the identification of bank customers for purposes of section 326 of the USA PATRIOT Act, could harm consumers and national interests.

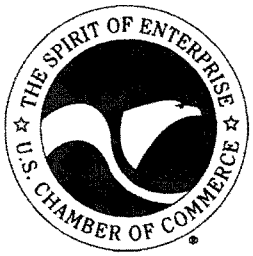
Finally, while we believe that H.R. 3997 is an important step towards resolving the problem of security of information about consumers, some issues raised by H.R. 3997 still require further resolution. For example, the harmonization provisions for GLBA section 501(b) rules may inadvertently leave the statute open to interpretation that the state insurance authorities may (or are even directed to) promulgate rules under GLBA section 501(b) relating to data security and investigation and notification of security breaches, inadvertently jeopardizing the critical goal of national uniform standards. Also, there continues to be some concern relating to the breadth and clarity of the trigger for investigation notices. Details, such as the need for notification to the United States Secret Service for breaches involving only a single consumer, or a few consumers, and clarification as to which insurance authority will be the "appropriate functional regulator" for insurers doing business in 50 states, may suggest a need to modify the current notification language or prompt regulatory attention under the exception authority that is already included in H.R. 3997. In addition, there is concern with the fraud mitigation provisions and the proposed specificity and standardization of notices. Other issues will undoubtedly arise during the legislative process.

Further, it is important to remember that regulatory compliance costs fall disproportionately on smaller financial institutions. Any legislative solution to data security and security breach notification must consider these and other costs that would be imposed on these institutions and their customers.

CONCLUSION

Financial institutions are proud of their record in protecting sensitive information relating to their customers. While we recognize that new regulatory requirements inevitably entail changes to existing practices, however sound, as well as additional costs, we will be pleased to continue to work with the Subcommittee to ensure that information about consumers is protected appropriately.

Thank you. I will be happy to answer any questions that you may have.



Statement of the U.S. Chamber of Commerce

ON: **"THE FINANCIAL DATA PROTECTION ACT"**

TO: **HOUSE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT**

BY: **KARL F. KAUFMANN**

DATE: **NOVEMBER 9, 2005**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

STATEMENT OF KARL F. KAUFMANN
SIDLEY AUSTIN BROWN & WOOD LLP
ON BEHALF OF THE UNITED STATES CHAMBER OF COMMERCE

Hearing on H.R. 3997, the Financial Data Protection Act
Before the Subcommittee on Financial Institutions and Consumer Credit

November 9, 2005

Good morning Chairman Bachus, Ranking Member Sanders, and members of the Subcommittee. My name is Karl Kaufmann and I am an attorney in the Washington, DC office of the law firm Sidley Austin Brown & Wood LLP. I am pleased to appear before you this morning on behalf of the United States Chamber of Commerce. The Chamber is the world's largest business federation, representing more than 3 million businesses of every size and in every sector of the economy.

In General

Mr. Chairman, the Chamber supports your effort, and the efforts of others on the Subcommittee, to develop legislation to protect the sensitive information of consumers. This morning I intend to discuss some of the key themes important to the Chamber with respect to data security and consumer protection. First, Congress should require that companies have reasonable programs to safeguard consumers' sensitive personal information, similar to the requirements imposed on financial institutions under the Gramm-Leach-Bliley Act ("GLBA"). Second, we believe it is appropriate for a company, upon discovery of a data breach, to notify consumers if their sensitive personal information has been acquired by an unauthorized person in a manner that presents a significant risk of harm to the consumers. If Congress decides to require additional consumer remedies in the wake of a data breach, we strongly urge Congress to recognize the different types of information that can be compromised and the different types of harm that can result. The Chamber also urges Congress to review the criminal penalties associated with hacking to determine whether additional penalties are necessary to deter and punish those who seek to obtain sensitive consumer information. Finally, and perhaps most importantly, any law passed by Congress must establish a national uniform standard with respect to information security, customer notification, and other related issues. This national uniform standard should be enforced solely by the appropriate federal agencies.

In general, the Chamber believes that H.R. 3997, the Financial Data Protection Act, approaches the above principles in a reasonable manner and therefore provides a sound framework for development of stronger consumer protection. We also understand that the legislation continues to evolve and that it may require additional refinement. We applaud you and the bill sponsors for establishing an open process to receive feedback from all interested parties, a process that began during the early developmental phases of the legislation. Such a constructive process has the potential to result in legislation which can gather broad support. The Chamber looks forward to continuing to work with you,

Mr. Chairman, and others to continue to shape this complex bill as it moves through the legislative process.

Information Security

Protecting consumers sensitive personal information is a priority for companies holding such information. We believe that the vast majority of companies who possess sensitive personal information take reasonable procedures to safeguard that information. There are strong market forces in place to encourage companies to protect information because the reputational and economic harms associated with a data breach can be severe. However, it takes only a few mistakes by a few companies to damage consumer confidence in the ability of all companies to protect sensitive information. Therefore, we believe it is appropriate to require companies that possess sensitive personal information to have reasonable procedures in place to protect the integrity and security of such information.

The Chamber believes that the information security requirements established under the GLBA for financial institutions should serve as a blueprint for the requirements that should apply to other companies that possess sensitive personal information. In this regard, the GLBA standards provide financial institutions with a risk-based approach to information security, requiring that programs be appropriate to the company's size, complexity, and activities. The Chamber believes that the information security requirements included in H.R. 3997 establish a data protection regime that takes a risk-based approach, recognizing that a "one size fits all" solution for companies of varying sizes and complexity is inappropriate. We commend the sponsors of H.R. 3997 for establishing such a framework and urge that this approach be retained.

Consumer Notification

Although companies implement reasonable security programs, and H.R. 3997 mandates such programs, there is no such thing as the "perfect" security program. Unfortunately, there will be occasions on which unauthorized individuals obtain sensitive information about consumers. We believe that consumers should be notified of certain security breaches in order to take appropriate steps to protect themselves from harm.

There are several issues which must be decided in connection with notifying individuals about security breaches. For example, what is a "security breach"? Such a definition is critical because it sets the baseline of circumstances for when consumer notices may be required. If the definition is too broad, consumers may receive notices when they are not necessary. If it is too narrow, consumers may not receive notices when they would be appropriate. The Chamber believes that a security breach in the context of the legislation is an event when an unauthorized individual acquires sensitive consumer information. This is similar to how H.R. 3997 defines a security breach.[1]

---

[1] We note that the legislative definition also includes "an unusual pattern of use of [sensitive consumer] information indicative of financial fraud." This prong of the definition may cause unintended

Although the definition of a security breach is important, it is not the only factor in determining whether a consumer should be notified of the breach. A critical factor is whether or not the breach, once discovered, is likely to result in substantial harm to an affected consumer. Only when the consumer is at risk for substantial harm will such a notice have true meaning to the consumer. For example, if a phone book publisher realizes that crates of undelivered phone books were stolen from its warehouse, it does not seem reasonable that the publisher should notify each of the consumers listed in the phone book of the "breach". This example is illustrative for two reasons. First, the information—name, address, and phone number—is not sensitive insofar as it is not of the type that would allow someone to commit fraud in the individual's name. Second, even if name and address were sufficient to commit fraud, the breach itself is unlikely to be the cause of substantial harm to the consumer because the phone books are available virtually anywhere. As a result, to "notify" consumers that the information in the phone book has been breached would be entirely unnecessary. Moreover, if consumers tend to receive notices of technical "breaches" that do not pose significant risks to consumers, such as a notice describing a breach at the phone book publisher, consumers may begin to ignore security breach notices. If this occurs, the goal of using consumer notices to inform the consumer of the breach, the consumer's rights, and how the consumer can protect him or herself is defeated.

Therefore, if we are to protect consumers properly, it is absolutely critical that consumers receive notices only when: (i) sensitive information is breached; and (ii) the breach is likely to result in substantial harm to consumers. If breach notices are limited to these circumstances, in the unfortunate instance when a consumer receives such a notice, it is much more likely that the consumer will be aware that the notice is important and should be read closely. The sponsors of H.R. 3997 appear to agree with the Chamber's view on this key issue. The trigger in the legislation is designed to ensure that notices are sent to consumers only when they would be meaningful, a concept the Chamber strongly supports.

We believe that there are several factors that should be taken into account when determining whether a consumer is at risk of substantial harm as a result of a breach. For example, very sensitive information could "fall into the wrong hands," yet if the information is protected by strong encryption the consumer is unlikely to be at risk of any harm at all. In fact, the Chamber would support efforts to deem the unauthorized access of encrypted information as unworthy of consumer notice, similar to an approach taken in California and other states. At the very least, data encryption should be a factor in determining whether the consumer may be harmed as the result of a breach. We also agree with H.R. 3997 that certain circumstances simply do not rise to level of requiring a notice, such as if a credit card account is closed and the card is reissued.

Mitigation of Harm

---

consequences, as many entities have programs to detect unusual patterns of information usage which are not indicative of a data breach.

The legislation requires companies to provide consumers with free access to credit file monitoring services for a period of time in certain circumstances. In particular, if the consumer is at risk of becoming a victim of identity theft as a result of a security breach, the breached entity must make available free credit file monitoring services for six months. Although consumers who are potential identity theft victims could access their credit report up to six times a year at no charge under current law, we believe that additional statutory mitigation may prove appropriate under the limited circumstances specified in the legislation. In particular, the Chamber is pleased that the bill distinguishes situations in which consumers may become victims of identity theft, and therefore may have reason to monitor their credit file, from situations where consumers may become victims of credit card account fraud for example. Although we fully recognize the impact of fraud on consumers and others, credit file monitoring is not a tool used to remedy credit card account fraud. In this regard, misuse of a credit card account without misuse of the accountholder's identification information will not be reflected on the consumer's credit file. Rather, if the transaction is not blocked by anti-fraud networks, the consumer would be alerted of the fraud via the periodic credit card statement. Of course, the major credit card companies voluntarily provide zero liability for those fraudulent transactions.

National Uniformity

The Chamber believes it is imperative for Congress to establish a set of national uniform standards pertaining to data security and related issues. This is an absolutely essential consumer protection, and we applaud its inclusion in the Financial Data Protection Act. Today there are approximately 20 different states that have laws relating to consumer notification of data breaches. The number of state laws is certain to increase within the next few months.

The proliferation of similar, but ultimately different, state laws with respect to information security issues is not in consumers' best interests. Varying notification standards can result in consumer confusion and inconsistent compliance with the law. Furthermore, the net result is that the states that require notices in the most circumstances will dictate national policy with respect to data breach notification requirements. Companies that operate on a nationwide basis cannot efficiently develop 50 different data breach notification compliance plans in addition to a federal plan. Such companies are likely develop a compliance plan that complies with the most onerous state laws, even if it results in "overcompliance" by sending more notices than required in the majority of other states. This result undermines one of the fundamental concepts included in H.R. 3997, that consumers receive notices only when they are meaningful. The result may also undermine the will of the majority of state legislatures that sought to limit unnecessary notices, but were "overruled" by a minority of states that pursued a different, and flawed, policy objective. We do not believe these types of outcomes are best for consumers. We also believe Congress is in a better position to establish national policy on this inherently interstate issue.

If there is to be a national uniform standard, there must be a national uniform interpretation of that standard. The Chamber is pleased that the Financial Data Protection Act is enforceable solely through administrative enforcement by the appropriate federal agencies. A federal law subject to interpretation by state enforcement agencies or trial attorneys is not truly a national uniform standard.

Deterring Computer Crimes

We believe that the criminals who obtain sensitive personal information in an unauthorized manner should be deterred from their crimes and punished severely. Therefore, the Chamber strongly endorses efforts to provide more resources and tools to law enforcement to investigate and prosecute data security crimes. We endorse increasing the appropriate criminal penalties, both to deter and to punish those who attempt to hack into a computer system. We believe a key component of protecting consumers is ensuring that law enforcement is properly engaged, even if the hacker's attempts were thwarted by strong data security programs.

Conclusion

The Chamber strongly supports many of the concepts addressed in H.R. 3997, the Financial Data Protection Act. We believe that, if properly implemented, these concepts will result in stronger consumer protections. In particular, it is important that companies that possess sensitive consumer information implement reasonable procedures to protect that information. In the event of a security breach which is likely to result in substantial harm to the consumer, affected consumers should receive appropriate notices. In order to ensure consumers receive the appropriate protections, Congress should establish a national uniform standard with respect to issues relating to H.R. 3997. The Chamber recognizes that the Financial Data Protection Act is still subject to further discussion. Mr. Chairman, we look forward to working with you and others to improve H.R. 3997 as it moves through the legislative process. Given the complexity of the legislation, it is extremely important that the legislative language reflect the true congressional intent. Thank you for the opportunity to testify this morning, and I would be happy to answer any questions.

Statement of Mr. H. Randy Lively, Jr.

CEO and President of the American Financial Services Association.

Testimony Before the House Financial Services Committee

November 9, 2005

Chairman Oxley, Ranking Member Frank and Members of the Committee,

I am H. Randy Lively, Jr., the CEO and President of the American Financial Services Association located here in Washington, DC. It is my honor and pleasure to be here this morning to testify in support of HR 3997, the Financial Data Protection Act of 2005, introduced by Representatives LaTourette and Hooley and cosponsored by a broad bipartisan array of Members of this distinguished committee.

The American Financial Services Association represents the nation's market rate lenders providing access to credit for millions of Americans. AFSA's 300 member companies include consumer and commercial finance companies, "captive" auto finance companies, credit card issuers, mortgage lenders and other financial service firms that lend to consumers and small businesses. I am proud to say that next year, AFSA will celebrate its 90th birthday as the nation's premiere consumer and commercial credit association.

As I mentioned at the outset, I am pleased to be here this morning to speak in support of the Financial Data Protection Act and ask you, Mr. Chairman, to have the committee give it expedited consideration. AFSA and its members believe that well informed, proactive consumers are our best defense and our first line of attack in protecting all of us from the dangers of identity theft.

According to the Federal Trade Commission, identity theft robs the nation of more than $50 billion annually. Consumer losses account for about $5 billion of the total and business absorbs the remaining $45 billion. Yet in addition to the immediate monetary loss suffered, AFSA companies are more concerned about losing the trust of treasured customers, and mishandling a security breach can cost us valued customers.

Obviously, the best way to protect our customers' information is to prevent a security breach from occurring in the first instance. Toward that end, we are focusing on training our own employees in the handling of sensitive personal information, and are scrutinizing the practices of third-party vendors who store or dispose of data which may contain personal financial information. There is no doubt that the industry needs to regularly upgrade and improve the practices and procedures of our own companies and our storage and disposal vendors to prevent security breaches from ever occurring in the first place.

AFSA member companies share this committee's goal of wanting to ensure American consumers that their personal information is safely protected. To accomplish this goal, AFSA members are regularly improving their security measures and procedures to prevent threats to their information systems. HR 3997 provides a clear and concise framework for AFSA's member companies and other financial service providers to follow in the unfortunate event of a data breach.

The authors of the Financial Data Protection Act of 2005 clearly understand that an effective breach notification and reaction system must be based on the real risk to the customer and the businesses that rely on the integrity of the data. If the breach notification system is overly broad

we run the risk of inundating our customers with notices and having them ignore important information they need to protect themselves.

HR 3997 establishes a reasonable and balanced approach for businesses and regulators to prevent potential breaches of data security as well as uniform procedures to follow if one does occur. The legislation appropriately anticipates that some breaches may pose a significant risk of harm or inconvenience to consumers' identities, whereas others may not create a significant risk for the consumer. This distinction will enable businesses to maximize their vigilance over consumer data, apply law enforcement and regulatory resources where they are most needed and focus consumers' attention to take steps to protect themselves when they are truly at risk.

The Financial Data Protection Act of 2005 calls on business to conduct an immediate investigation if it is learned that a breach has occurred to assess the nature and scope of the breach. The investigation will determine whether the breach has created a substantial risk for the customers' personal financial information. The determination will take into account what information has been exposed and whether the information was encrypted, redacted or requires technology that is not commercially available. AFSA believes that the committee should direct the functional regulators to treat the breach of encrypted information as not creating a potential substantial harm unless an actual harm can be demonstrated. In other words, there should be a presumption that the acquisition of encrypted information does not create a substantial risk for consumers to whom the information relates.

Should a business determine that a substantial breach has occurred, HR 3997 directs a company to notify the Secret Service and the appropriate functional regulators as well as third parties that might be affected by the breach. This type of coordinated framework will ensure that ongoing law enforcement investigations are not compromised by premature publication of breaches. At the same time, the legislation provides reasonable parameters so that a delay in notifying consumers does not unnecessarily extend their exposure to risk of harm.

HR 3997 directs that breach notices to consumers must be done in a clear and conspicuous manner that describes the nature of the breach, when the breach occurred, the relationship between the consumer and the entity who suffered the breach, and actions that the business is taking to restore the security and confidentiality of the breached information. The bill also requires that the consumer notice includes a summary of rights the consumer has as a victim of fraud or identity theft. AFSA supports this approach because the legislation also recognizes that a notice that follows this format should only have to be given once.

AFSA whole heartedly agrees with the sponsors of HR 3997 in directing federal regulators to work together to create uniform security standards and policies for each business to implement and maintain to protect sensitive information. Moreover, a uniform national standard replacing the patchwork of varied and numerous state and local requirements will avoid needless duplication that could lead to confusion and divert resources from the actual problem.

I appreciate the opportunity to be here today and would be happy to answer any questions you may have.

Statement for the Hearing Record

Submitted By
ARMA International
To the

Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
U.S. House of Representatives
Washington, DC
Regarding its Hearing on

H.R. 3997, Financial Data Protection Act of 2005

November 9, 2005

Strong Public Policy is Needed to Protect Financial Data Security

Americans demand security and privacy of their personally identifiable information. The establishment of new systems that allow easy access and transference of personally identifiable data between parties should to be sensitive to personal privacy and grant assurance to Americans that their data will not be misused or end up in the wrong hands.

Incidents of breaches of personally identifiable information are on the rise. A 2003 survey of a one-year period by the Federal Trade Commission revealed that more than 10 million people had experienced identity theft in one form or another.[1] Widely-reported episodes of data breach, such as Bank of America and Lexis-Nexis, serve as lessons to information brokers that the highest level of security is required to ensure that personally identifiable information is not compromised. For these reasons, we appreciate the attention that policymakers are giving to this important issue.

Because of the essential role of effective and appropriate information management in today's economy, ARMA International has a strong interest in issues pertaining to safeguarding consumer information and other personally identifiable information possessed by business and government.

While ARMA International lauds efforts to address incidents of financial data breach, we believe that H.R. 3997 does not adequately address the prevention of data breaches. A records and information management program, dedicated as a written set of policies and procedures for the management of information in the custody of an organization, is just as essential an element of any data safeguard regime as are new technologies designed to enhance data security. Therefore, ARMA respectfully urges that the Subcommittee at a minimum enhance the safeguards provisions of H.R. 3997 by incorporating language into the measure directing that mandated data security policies and procedures be in writing and be made available to all personnel with access to sensitive financial information that the bill is intended to protect.

ARMA International's interest in congressional efforts to protect sensitive consumer information is based on our confidence of the role that a written records and information management program plays in maintaining an information security regime in any organization. A sound records and information management policy, guided by the best practices of the field of records management, can serve as an important tool to achieve the goal of securing personally identifiable financial data and preventing data breach. The application of a records and information management program is based on the goal of preserving the security and integrity of all records in the custody of an organization, protecting such records from unauthorized use, and properly disposing of such information appropriately at the end of a records' life cycle.

Once Congress acts to create an affirmative obligation by covered entities to protect the security of sensitive personally identifiable financial information, ARMA strongly

[1] See Federal Trade Commission Identity Theft Survey Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

recommends that any data security safeguards include a written program of policies and procedures designed to guide personnel throughout an organization and ensure that records are properly maintained, accessed and disposed of. A written program will also serve as a benchmark, not only for the organization and its leadership to ensure proper compliance with corporate expectations, but also as a guide for regulatory agencies given the responsibility of ensuring that companies do what they profess to do. Our belief in the role of an appropriate written policy also recognizes that no technology can completely address the human component involved in records management.

ARMA acknowledges that the best practices of records and information management are supported by a compelling business argument. A written program that is communicated throughout an organization provides the best defense for an organization should data breaches occur inconsistent with its own policies. But ARMA also acknowledges that not all organizations endorse the best practices of records and information management without external incentives. Legislation designed to protect financial data from unauthorized breach should also include meaningful sanctions when organizations do not put in place reasonable security measures designed to protect sensitive personal information. ARMA notes that H.R. 3997 contains no provisions that would allow regulatory enforcement agencies to impose sanctions upon bad actors who allow data breach to occur when security standards are lax. As currently written, H.R. 3997 provides no penalty for organizations that willfully or wantonly handle consumer financial information, thereby providing no incentive for a covered entity to ensure that the maximum level of security is maintained when handling information.

Why Records and Information Management is Important for Data Security

Information is among the most valuable commodities of any organization. In the case of organizations that possess, process, and use sensitive consumer information, this information is a part of the organization's strategic business model. As such, these organizations have a significant responsibility to manage and maintain the integrity and security of this information, including the implementation of appropriate safeguards against unauthorized use and the proper disposal of the information.

"Records management" is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.[2]

Of primary importance from a records and information management perspective is ensuring the integrity and security of information. Whatever information management systems are in place must ensure protection of the records and information in these two critical areas. Public sector agencies and private sector entities should not have access to personally identifiable information unless the information is essential to the organization's work. It is important that public and private sector entities identify what

[2] See "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"), p. 3.

information is actually mission critical, who within their organizations should have access to the information, and then ensuring that the information cannot be accessed by unauthorized parties. It is the role of a written information management program that informs all employees within an organization of any routine protocols for business records as well as special protocols for legislatively mandated safeguards.

ARMA notes that a significant risk of identity theft occurs at a point when a given record should be destroyed – and the best practices of records and information management and a record's retention schedule would require not only appropriate measures to ensure destruction, but also the documentation of the destruction or final disposition action.

Within the context of managing the life cycle of any information, assuring that records and information are destroyed appropriately – at the time and in the manner anticipated by the organization's retention and disposition program, and in compliance with any applicable law or regulation – is as important and deserves the same level of attention and stewardship as assuring that the information is properly maintained. The appropriate destruction of a record at the end of its life cycle will assist with efforts to secure personally identifiable information and curb identity theft. The same best practices will safeguard the misappropriation of records stored in electronic format.

Records and information management policies provide a guideline for the creation, use, maintenance, and disposition of a record in the ordinary course of business. An appropriate records and information management program in an organization includes setting policies and standards, assigning responsibility and authorities to particular individuals within an organization, establishing procedures and guidelines, providing a range of services relating to the management and use of records, designing, implementing and administering specialized systems for managing records, and integrating records management into business systems. Records contain information that is a valuable historical resource and an important business asset.[3] "A systematic approach to the management of records is essential for organizations and society to protect and preserve records as evidence of actions. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders."[4]

A records management policy empowers organizations to conduct business in an orderly, efficient and accountable manner, deliver services in a consistent and equitable manner, support decision making by organizational management, provide continuity in the event of a disaster, and meet legislative and regulatory mandates including archival, audit and oversight activities. A vigorous program will also provide protection and support in litigation including the management of risks associated with the existence of, or lack of, evidence of organizational activity, protect the interests of the organization, support

---

[3] See "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"), p. 4.
[4] Ibid.

current and future research and development activities, and assist with maintaining organizational memory.[5]

ARMA believes that any security regime for personally identifiable information should include support by senior management of a written records and information management program.[6] This would include the appropriate investment in personnel, training and organization-wide communications. It would also ensure that third party relationships endorse the same safeguards with appropriate means of ensuring compliance.

In today's distributed work environments, a wide variety of individuals create records and must therefore take responsibility to ensure those records are captured, identified and preserved. It is no longer enough to train administrative staff and assume they will make sure the records end up in the records management program. All members of management, employees, contractors, volunteers and other individuals share the responsibility for capturing records so they can be properly managed and secured throughout the length of their required retention period. An appropriate records management program includes a risk assessment program which includes conducting a physical site survey, identifying probable threats to records, including the systems vulnerability to deliberate destructive acts.[7]

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) contained a provision that required the Federal Trade Commission and the various banking regulators to develop a disposal rule for sensitive customer information. This rule may provide a model for businesses in other industry sectors for the appropriate disposal of personally identifiable information. In comments[8] to the disposal rules proposed by the Commission and the various banking regulators, ARMA strongly recommended that an organization's safeguards include a formal, written records and information management program.

About ARMA International

Established in 1956, ARMA International (ARMA) is the non-profit membership organization for the records and information management profession. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, technologists, legal administrators, librarians, and educators employed by both private and public institutions. Our mission includes providing education, research, and networking opportunities to information management professionals, as well as serving as a resource to public policy makers on matters related to the integrity and importance of records and information.

ARMA serves as a recognized standards developer for the American National Standards Institute (ANSI), participating and contributing toward the development of standards for

---

[5] Ibid.
[6] "Requirements for Managing Electronic Messages as Records," P. 3
[7] "Records Programs: Identifying, Managing, and Recovering Business-Related Records" , p. 4.
[8] ARMA's comments on the disposal rule may be viewed at http://www.ftc.gov/os/comments/disposal/index.htm.

records and information management.[9] ARMA is also a charter member of the information and documentation subcommittee of the International Organization for Standardization (ISO), aiding in the development of its records management standard, ISO 15489.[10]

Records and information management plays an important role in the private and public sectors. In this new century, the most valuable commodity of business is information, often in the form of data bases of essential information required by the service sectors of our economy. The greatest responsibility for organizations will be managing and maintaining the integrity of an ever-growing flow of information, including the establishment of appropriate safeguards for sensitive information and in establishing retention schedules complaint with regulatory and statutory requirements. These challenges call for increased recognition of the role of managing critical information and providing appropriate protections for personally identifiable information. Organizations that embrace information management as being strategic and mission critical will ensure their competitive advantage and remain appropriate stewards of information containing sensitive consumer information. Maintenance of an appropriate records and information security program provides numerous benefits, including efficiency, accessibility, and security.[11]

Conclusion

ARMA International applauds the Subcommittee for examining the issue of securing personally identifiable financial information. ARMA recommends that any effective data security initiative include a vigorous records and information management program, informed by written set of policies and procedures, communicated throughout the organization, and supported by senior management, to help ensure that breaches of security do not take place.

Respectfully submitted,
Cheryl L. Pederson, CRM
President
ARMA International
13725 W. 109th St., Suite 101
Lenexa, KS 66215
800.422.2762/913.341.3808
Fax 913.341.3742

---

[9] "Managing Recorded Information Assets and Resources: Retention and Disposition Program" may be viewed at http://www.arma.org/standards/public/document_review.cfm?DocID=22.
[10] "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"). ARMA fully supports ISO 15489-1.
[11] "Records Center Operations", p. 1.

Written Testimony of ID Analytics Corporation

Before the Subcommittee on
Financial Institutions and Consumer Credit

Hearing on H.R. 3997,
the "Financial Data Protection Act of 2005."

Washington, DC
November 9, 2005

Mr. Chairman, Ranking Member Sanders, and other distinguished members of the Subcommittee on Financial Institutions and Consumer Credit, ID Analytics is pleased to submit for your consideration a summary of relevant findings from its forthcoming "National Data Breach Analysis."

We are submitting written testimony, even before the study is publicly released, because we believe the Committee should have the best evidence available as it ponders legislation with respect to how criminals are using (or not using as the case may be) information obtained from data breaches.

By way of background, ID Analytics is a San Diego-based company that provides Identity Risk Management solutions to a number of the nation's largest financial institutions, credit card issuers, and wireless companies. ID Analytics is in a unique position to offer insight into the data breach problem because of our analysis of the "breached files" of three highly publicized data breaches involving hundreds of thousands of identities.

This analysis was conducted using ID Analytics ID Network, a nationwide, cross-industry collaborative fraud prevention system. ID Network Members are organizations that contribute consumer identity elements sourced from their customer management processes, including account applications, requested changes of account information, and tendered payments, in the interest of collectively preventing identity theft and related fraud. Each ID Network Member has agreed that identity fraud prevention requires a new level of collaboration and has entrusted ID Analytics to develop and maintain the technology required for comprehensive and effective Identity Risk Management.

For the purposes of this research, ID Analytics classified each breach as either an "identity level" or "account level" breach. An identity level breach involves the most sensitive data available – names, Social Security Numbers (SSNs), dates of birth, addresses, and other personally-identifiable information. An account level breach involves mostly account data such as credit card numbers and credit card expiration dates.

Summary of Findings:

During the summer and fall of 2005, ID Analytics conducted an analysis of the breach files of three widely-publicized data breaches involving hundreds of thousands of consumer identities. The primary purpose of this analysis was to determine the degree to which identity fraud results following a data breach.

One of the breaches analyzed involved a serious breach of identity-level information on consumer reports. Two of the breaches involved the disclosure of account-level information on credit card accounts. Selected key findings are as follows:

- **ID Analytics' analysis of the identity-level breach, which involved over 100,000 consumer identities, revealed the following:**
  - Misuse of the breached identity information began gradually, spiked around the discovery of the data breach and declined precipitously after the breach was publicly announced.
  - Fraudsters used identity data manipulation, or "tumbling," to avoid detection and prolong the scam.
  - The calculated fraudulent misuse rate for consumer victims of the breach was 0.098%. This rate is less than the annual rate of identity fraud for all Americans reported by the FTC Synovate report in September 2003.
- **ID Analytics' analysis determined that the two account-level breaches did not indicate patterns of new fraudulent activity.**
- **Technologies now exist that can measure the fraud risk associated with breached identities and results are being proven.**

Study of the Targeted Identity Breach:

In mid-2005, ID Analytics was approached by an ID Network Member and asked to explore opportunities to use the ID Network and its associated technology to determine if identity fraud was resulting from a well-publicized data breach of an unaffiliated third party.

The data breach in question was what ID Analytics considers a "targeted breach," meaning there was a deliberate theft—or hacking—of data. It was also what we call an identity level breach as the data stolen consisted of more than 100,000 consumer identities, including Social Security Numbers, dates of birth, names, and other sensitive information. ID Analytics' scientists and fraud analysts set to work to determine if the breached data was being fraudulently misused and, if so, to propose a strategy for preventing any further identity fraud resulting from the breach.

ID Analytics did, in fact, discover fraudulent misuse associated with this major data breach. While we will not go into great detail about the science and analysis used to discover the fraud, we will attempt to explain the basic method.

The underlying theory was that identity information associated with a breached file should not exhibit suspicious patterns and relationships unless that information was being misused in an organized manner, as in the case of a fraud ring perpetrating identity fraud.

Under normal circumstances, any two identities should exhibit subtle, but not suspicious, relationships to each other. For example, husbands and wives cohabitate, and thus share addresses and telephone numbers. Two random individuals can even share the same names, and thus their identity data "relates" in an innocuous manner. Yet two previously unrelated identities should not suddenly begin sharing SSNs, addresses, or telephone numbers. Such suspicious relationship patterns become evident as the identity is asserted on subsequent new account applications; these patterns can be indicative of identity fraud in action. In isolation, many of these patterns appear safe, but with an extremely wide perspective and through millions of repeated observations, sophisticated analytical technology can help interpret suspicious patterns, such as those associated with a data breach that is resulting in identity fraud.

ID Analytics' analysis of the breached file yielded the following results:

(1) Roughly 1 in 1,020 breached identities (0.098%) were used to commit identity fraud. This rate is less than published reports about the annual rate of identity theft affecting the general population.

This rate of fraud in a breach population, called hereafter the "misuse rate," speaks to an important truth about identity-level breaches. Practical constraints, and not the size of an identity-level data breach, determine the amount of identity fraud that is likely to result from a data

breach. It is the fraud ring's available resources that determine how much fraud follows a targeted, identity-level data breach. Fraud rings simply do not have the time or manpower to use hundreds of thousands of identities available to them in their nefarious pursuits.

While initially surprising, these seemingly low use rates from data breaches, upon further consideration, appear rational. Assume the following:

- Five minutes to fully and accurately complete a new account application that is likely to be approved
- One application per unique identity
- Average 6.5 hours per work day, five days per week, 50 weeks per year

Given the above constraints, it would take on individual fraudster over 10 years to fully utilize a breached file consisting of one million consumer identities. Should the fraud ring outsource these tasks at a rate of $10 per hour in an effort to fully utilize the breached file within one year, the fraud ring would have to hire 52 workers and spend over $830,000. This scenario also overlooks other practicalities, such as procuring the applications, logistics around receiving loan instruments (credit cards or loan checks), and the need to launder the proceeds of the fraud. These practicalities imply that there exists a feasibility limit associated with fraudsters committing identity fraud using breached identities.

However, misuse rates could continue to increase drastically over time if the vibrant black market for "identities" remains unimpeded. Today, there is no evidence of a central, thriving, continuously-operated black market, although there is evidence that some stolen consumer data is sold via internet relay chat (IRC) networks and through other internet-based communications channels. By selling any amount of the remaining identities (those not able to be used because of the "feasible limit"), fraud rings could maximize the proceeds from their efforts and exact a far greater degree of harm to consumers, industry and government over time. It should be clear that this scenario calls for consortium-based, real-time, identity-centric technology solutions to prevent ensuing identity fraud.

(2) Fraudsters used identity data manipulation, or "tumbling," tactics to avoid detection

ID Analytics' scientists observed that the fraudsters misusing the consumer identities associated with this data breach were engaging in creative tactics to prolong the scam and avoid detection.

Figure 1: Evidence of Identity Data Manipulation, or "Tumbling" Over Time

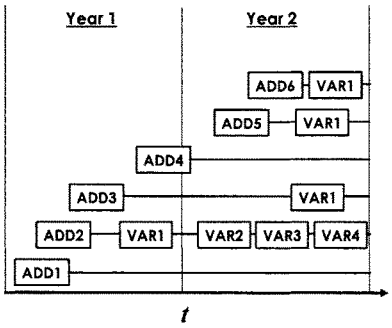
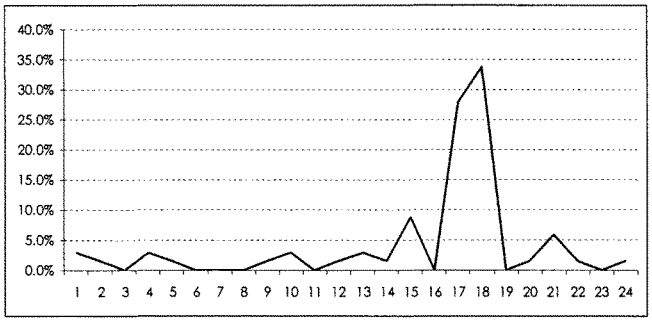


Figure 1 provides evidence of one such technique that has been referred to as "tumbling." The fraud ring in this example chose to manipulate the addresses submitted as part of the account applications over time, resulting in obscure, yet difficult-to-detect variations of the original address. The manipulations illustrated here amounted primarily to changes in apartment numbers or spellings of street names. Interestingly, scientists observed a dramatic increase in these manipulations in the latter days of the identity fraud scam.

(3) Misuse of the breached identity information began gradually, spiked around the discovery of the data breach and declined precipitously after the breach was publicly announced

Over the 24-month observation window for this data breach, there was a 12-month pattern of low rates of misuse followed by a brief 6-month period of a high rate of identity use, and then a steep reduction in identity use after 18 months.

Figure 2: Monthly Identity Use Rate for Selected Data Breach



The increased rate of misuse began around month 14. This elevated rate of misuse lasted for months and dropped off precipitously when the breach was announced around month 22.

ID Analytics can only speculate on this rate of misuse by the fraudsters responsible for this particular data breach. One possible answer is that the fraudsters were using the identities sparingly in order to avoid detection. Around month 14, when the breach was discovered by the commercial entity, the fraudsters may have realized the game would soon be up and tried to maximize the cash value of the data in their possession. Once the breach was announced, the misuse of the identities fell precipitously. We do not know at the time of this study whether the identities will be further misused in the future, but continued monitoring would be required to make such a determination.

Study of Account Level Breaches:

If identity fraud does result following an account level breach, the lasting effect to the consumer involves unwinding this damage through a rigorous series of calls to credit reporting agencies, the issuing lender, and any number of police departments (depending on jurisdiction).

But account-level data breaches can lead directly to credit card transaction fraud. In contrast to identity fraud, where identity elements of a consumer are typically used to perpetrate financial fraud across

numerous cards and accounts, credit card transaction fraud by contrast involves just using a particular credit card to perpetrate fraud. This type of fraud does not burden the consumer as much, nor does transaction fraud persist after the institution takes appropriate measures since either the merchant or the card issuer bear the financial losses resulting from the fraud.

Since account-level data breaches generally involve the disclosure of credit or debit card numbers, expiration dates, and names, when the institution reissues the account number and invalidates the compromised one, transaction fraud is prevented for that victim. Most institutions assume 100% of the liability in these cases of fraud where identity fraud is not a concern because a name alone is not enough information by which to commit identity fraud.

However it is theorized that account-level data breaches can lead to identity fraud if a new account is (or multiple accounts are) opened in the victim's name. Logically speaking, if a fraudster obtained a name and a credit or debit card account number, he could use the internet to "find" the victim and steal the other necessary information (SSN, date of birth, etc.) to perpetrate identity fraud on new account applications or to access existing accounts and defraud the victim.

ID Analytics was approached by an ID Network Member to seek an answer to the following question: **Does a fraudster who accesses an account-level data breach file have the intent or ability to gather additional identity information on the breached identities in an effort to perpetrate follow-on identity fraud?**

This ID Network Member provided ID Analytics with two separate account-level breached files. Both of the breached files originated from US-based retailers' computerized account databases that had been accessed illegally. ID Analytics conducted analyses on both files, but presents results for this report in the aggregate.

While the hackers responsible for the breach did not have consumer identifying information other than name, account number and expiration date, the ID Network Member appended that identity information to the file in order to determine if there was any attempted identity fraud following the breach.

ID Analytics' analysis of the breached file yielded the following results:

(1) No Widespread Fraud Patterns Detected in the Account Level Breach

There was no evidence that the breached file was being exploited by fraudsters to perpetrate large-scale identity fraud scams. While there was one account-level fraud attempted out of 1428 breached accounts (one account level breach above the average misuse rate of 0.07% and one below the average rate of misuse), we found that there was no evidence that follow-on identity fraud had been perpetrated against the two breached account level populations.

(2) Identities from the account-level breach file exhibited an unsuspicious distribution of Social Security Number relationships to reported fraud when compared to a control group.

The table below compares the percentage of fraud hits found by SSN within the ID Network.

Table 1: Social Security Number Relationships to Reported Fraud

Number of SSN Relationships to Reported Fraud	Account Level Breached Group	Control Group
None	99.38%	99.12%
1 fraud hit by SSN	0.61%	0.86%
2 fraud hit by SSN	0.01%	0.02%
3 or more fraud hits by SSN	0.00%	0.01%

As Table 1 illustrates, identities from the account-level breach file exhibited an unsuspicious distribution of SSN relationships to reported fraud when compared to the control group. Both this account-level breach file, as well as the identity-level breach file actually appeared safer than the control group on this SSN-only dimension.

Table 2: Comparison of Anomalous Address Links

Number of Anomalous Relationships by Valid Address	Account Level Breached Group	Control Group
>4	0	1
4	0	0
3	0	1

Table 3: Comparison of Anomalous Telephone Relationships

Number of Anomalous Relationships by Valid Phone Number	Account Level Breached Group	Control Group
>4	0	0
4	0	0
3	0	0

As Tables 2 and 3 indicate, the account-level breach file exhibited no suspicious relationships to either addresses or telephone numbers, indicating an extremely low probability that the affected consumers will become victims of identity fraud.

ID Analytics conducted many other tests on this data set and believes that consumers affected by this account-level data breach will not fall victim to identity fraud in any significant numbers.

Conclusion:

ID Analytics recognizes that the information provided by these three breach analyses is only the beginning of our understanding of how criminals are capitalizing on data breaches to perpetrate fraud.

We appreciate the opportunity to express our views and would welcome the opportunity to more fully brief the Committee on the findings of our study.

Sincerely,

Mike Cook
Vice President
ID Analytics

STATEMENT

of Kurt Pfotenhauer for the

Mortgage Bankers Association

on

"The Financial Data Protection Act of 2005"

for the

Subcommittee on Financial Institutions and Consumer Credit

United States House of Representatives

November 9, 2005

Thank you for allowing the Mortgage Bankers Association (MBA)[1] the opportunity to submit a Statement for the Record for the hearing on H.R. 3997, the *"Financial Data Protection Act of 2005."* This legislation, as an amendment to the Fair Credit Reporting Act (FCRA), would mandate a national standard for the protection of consumer information and require institutions to provide notifications to consumers in the event that an investigation determines that a data security breach has occurred or is reasonably likely to occur.

MBA understands the importance of providing effective protection of the sensitive financial information of consumers, and supports legislation that makes this protection possible. MBA believes that, with modifications, the passage of the H.R. 3997 could put in place legislation that would allow for a clear, consistent and uniform set of guidelines by which financial organizations can implement data security programs and policies that better protect consumers from the expanding threat of identity theft.

MBA's Involvement in Data Security

MBA works with its members on developing policy positions (and associated standards and best practices) on information technology. MBA member activities, such as loan origination, closing and servicing require the collection, processing, transfer, storage and disposal of private information. Personal data elements are critical assets for risk assessment within the primary mortgage market.

MBA has a long and active history of supporting technology initiatives, including the Financial Institution's Electronic Data Interchange (EDI) in the early 1990s and the establishment of two entities that support data integrity: the Mortgage Industry

[1] The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 500,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership and extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 3,000 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, Wall Street conduits, life insurance companies and others in the mortgage lending field. For additional information, visit MBA's Web site: www.mortgagebankers.org.

Standards Maintenance Organization (MISMO) [2] and Secure Identity Services Accreditation Corporation (SISAC) [3].

MISMO continues to press for innovation in the mortgage process by providing a specification for electronic mortgages (eMortgages), codifying a single location for the registry of authoritative electronic notes and establishing federated identity management policy for authentication.

Confidentiality, integrity and non-repudiation have been recognized within the industry as critical principles for electronic records and signatures. For many years, MBA has been addressing information security as a unique discipline. SISAC was established in 2003 to address these security principles. SISAC guidelines are for medium to high assurance levels corresponding to risk associated with mortgage transactions. The framework for SISAC was industry and government best practices including: the Federal Public Key Infrastructure (PKI) Bridge, National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), as well as other well-known standards organizations. MBA is well respected within the security domain as demonstrated by the election of MBA staff to the Electronic Authentication Partnership Board of Directors and by the selection of MBA to provide contract services to the General Services Administration (GSA) Office of Government-wide Policy.

A large number of MBA member companies are regulated by the Financial Regulatory Agencies ("the Agencies") – including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Securities and Exchange Commission, the Commodity Futures Trading Commission and the Federal Trade Commission. As such, these companies are currently required to comply with safeguarding provisions that have been mandated by the Gramm-Leach-Bliley (GLB) Act, and therefore, have existing measures in place for protecting the sensitive financial information of consumers.

MBA and its members have also been instrumental in advocating for consumer financial literacy. We encourage consumers to take advantage of accessing free credit reports, as provided by the Fair and Accurate Credit Transaction Act (FACTA), in order to

---

[2] The Mortgage Industry Standards Maintenance Organization, Inc. (MISMO), a not-for-profit subsidiary of the Mortgage Bankers Association (MBA), develops data transfer protocols that span the $9 trillion residential and commercial real estate finance industry. MISMO coordinates the development and maintenance of Internet-based Extensible Markup Language (XML) real estate finance specifications and electronic mortgage guidelines through a voluntary, open and vendor-neutral process, and its workgroups include more than 2,300 individual participants from over 160 subscribing organizations representing all sectors of the residential and commercial industry: lenders, originators, servicers, investors, government-sponsored enterprises, technology vendors, multiservice providers, credit reporting agencies, insurance firms, tax services and law firms. For more information on MISMO, visit www.mismo.org.

[3] The MBA's wholly owned nonprofit subsidiary Secure Identity Services Accreditation Corporation (SISAC) is responsible for accrediting digital identity credential issuers against industry standards for secure identities in the mortgage industry. More information can be found at http://www.sisac.org.

monitor their financial history and ensure that any unauthorized activity – namely identity theft – has not occurred.

MBA has advocated for a strong and effective information security network. We commend the House Subcommittee on Financial Institutions and Consumer Credit for its efforts to ensure the protection of sensitive financial information of consumers.

Background on Data Security

Data security refers to the secured storage of "personal identifying information," which is generally defined as a person's first name or first initial, last name, date of birth, address or telephone number, in conjunction with their Social Security number, driver's license number or account number or credit or debit card number combined with the access code (also known as a PIN number). Information may come from a variety of sources, such as an application (for a mortgage loan, car, etc.), a credit report or an account transaction history, and is typically not data that is publicly available. A "security breach" occurs when the personal identifying information of a consumer or consumers has been stolen or compromised.

Some companies collect personal identifying information and use it directly, for purposes such as extending credit, while other companies collect and store personal identifying information for use by third parties, such as credit reporting agencies. Whether companies directly use the information or store it for another party, they are required to have policies and procedures in place for safeguarding the information and protecting it from unwarranted access by outside parties.

Currently, GLB requires the Agencies to establish data safeguards standards for the financial institutions subject to their jurisdiction. The safeguards are to ensure the security and confidentiality of customer records and information, and to protect against any anticipated threats or hazards to the security or integrity of those records. The safeguards are also to protect against unauthorized access to, or use of the records or information, that could result in harm to the customer.

The Agencies have issued guidelines that establish standards for safeguarding customer information and are authorized to enforce these guidelines with respect to the financial institutions that fall under their jurisdiction.

Current Legislative Activity

Over the past year, there have been a number of cases involving personal information that was either accessed without authorization, improperly disclosed to third parties or lost via postal transmission. In response to this activity, Congress has held a series of hearings relating to the storage and protection of the personal identifying information of consumers. A variety of bills have also been introduced, at both the Federal and state level, that outline provisions for proper storage of personal information data and for notifying consumers when their information has been compromised.

As of today, 20 bills have been introduced in Congress concerning the protection of sensitive consumer information. At the state level, there are approximately 266 bills that have been introduced relating to the overarching issue of privacy. To date, 18 states have passed legislation requiring consumer notification of a breach of personal information and more than a dozen others have drafts pending.[4] These numbers are expected to increase.

Positive Features of H.R. 3997

H.R. 3997 is a bipartisan bill that would mandate a national standard for the protection of consumer information. It requires financial institutions to conduct investigations if they determine or become aware of information indicating that a data security breach has occurred or is reasonably likely to occur. If these investigations determine that a breach is reasonably likely to result in identity theft or account fraud, the institutions must provide notifications to consumers. Furthermore, if any institution issues notifications, they must also provide consumers with a free credit monitoring service for at least a 90-day period. The bill would be an amendment to FCRA.

MBA's review of H.R. 3997 has determined that the legislation contains a number of positive provisions that would implement data security standards while still allowing mortgage lenders to avoid additional regulatory burdens and continue serving the nation's consumers in the most efficient manner. Specifically these provisions would:

- Set a national standard for the protection of consumers' sensitive financial information. MBA supports this measure, as it will help lenders avoid the regulatory burden of staying current with an ever-changing patchwork of state and local laws. Uniformity would lower the cost of home financing, as lenders who operate in multiple states would have a single standard to apply. Furthermore, a national standard would mean that consumers need only understand one law when pursuing remedies for a data security breach. Precedence for Federal preemption has already been set with the passage of FCRA.

- Authorize the Agencies to develop standards and guidelines that would allow financial institutions an exemption from liability if, at the time of a security breach, an institution had reasonable policies and procedures in place for protecting the security and confidentiality of the sensitive financial information of consumers, and if free credit monitoring service is offered as a result of the breach. MBA believes such a provision would encourage financial institutions to further develop conscientious policies and procedures for safeguarding consumer information. MBA does seek further clarification on what would be considered "reasonable."

[4] Although Indiana is one of the 18 states, the law is applicable to state agencies only.

- Appropriately recognize GLB requirements by deeming financial institutions as in compliance with certain provisions of the bill, so long as such institutions are subject to and substantially in compliance with GLB. MBA supports legislation that considers GLB applicability, and is evaluating the bill to determine whether it provides enough coverage of GLB.

- Assign the responsibility of providing consumer notifications to the organization that suffers a data security breach. MBA agrees that ownership of a security breach should be directly assigned to the organization accountable for the breach. However, MBA also believes that legislation should clarify which entity will be responsible for the costs of providing consumer notifications in cases involving breaches of personal information that is stored, but not owned, by third party companies. Responsibility of all associated costs incurred when there is a breach, such as credit freezing and call-center operations, should be assigned directly to that organization regardless of the origin of personal information involved in the breach.

Other Issues Affecting Mortgage Lenders

Upon MBA's review of all the proposed Federal legislation and state bills that have either been proposed or passed, a number of other issues have emerged that could have a significant impact on the mortgage banking industry. MBA urges the consideration of the following issues in H.R. 3997:

- The development of agreeable and concise security breach triggers that will not cause lenders to be unnecessarily overburdened in providing notifications, especially if there is not a perceivable threat of identity theft.

- H.R. 3997 does not specify what form of data (paper or computerized) is covered in the definition of "sensitive financial identity information." MBA believes the bill should clarify the type of form for the sensitive information, in order to allow for consistent interstate commerce application.

Conclusion

MBA and its members understand that strong data security is crucial for the operation of our modern real estate finance system. As such, MBA supports legislation that provides protection for the personal identifying information of consumers. MBA believes that, with modifications, the passage of the *"Financial Data Protection Act of 2005,"* could put in place legislation that provides a clear, consistent and uniform set of guidelines and laws by which financial organizations can implement personal information protection programs and policies that better protect consumers from the expanding threat of identity theft.

We look forward to working with the Subcommittee on this legislation.

THE NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

STATEMENT

OF

THOMAS M. BOYD

COUNSEL

NATIONAL BUSINESS COALITION ON E-COMMERCE & PRIVACY

ON

H.R. 3997

THE FINANCIAL DATA PROTECTION ACT OF 2005

BEFORE

THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
FINANCIAL SERVICES COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

NOVEMBER 9, 2005

ACXIOM
AMERICAN CENTURY INVESTMENTS
ASSURANT, INC.
CHECKFREE
CIGNA
DEERE & COMPANY
EASTMAN KODAK COMPANY
EXPERIAN
FIDELITY INVESTMENTS
GENERAL ELECTRIC
GENERAL MOTORS
INVESTMENT COMPANY INSTITUTE
MBNA AMERICA
PROCTER & GAMBLE
CHARLES SCHWAB AND CO.

KIM QUISH
CHAIR

601 PENNSYLVANIA AVENUE, N.W.
NORTH BUILDING, 10TH FLOOR
WASHINGTON, DC 20004-2601 USA
202.756.3385
FAX - 202.756.3333

We want to thank Chairman Bachus, Ranking Member Sanders, and the Members of the Subcommittee for inviting us to submit written testimony to you as part of your hearing on H.R. 3997, The Financial Data Protection Act of 2005, and for working with us throughout the process on this important legislation.

My name is Thomas M. Boyd and I am a partner in the law firm of Alston & Bird, LLP. We are counsel to the National Business Coalition on E-Commerce and Privacy ("The Coalition"), a formal, non-profit corporation created in February, 2000. Comprised of seventeen brand name companies, the Coalition is a deliberately diversified organization committed to the adoption of balanced and reasonable national public policy in the area of electronic commerce and privacy. Our members, listed in the margin of this statement,[1] are both financial and non-financial companies and each of them is strongly

[1] J.P. Morgan Chase & Co. and MasterCard Incorporated are recent additions to the Coalition membership.

committed to ensuring the privacy and security of its customers, both online and offline.

In addition to our membership, we have worked informally with an equally diverse range of other companies, associations and groups for the collective purpose of serving as a positive resource to assist the Financial Services Committee and the Congress in its effort to forge legislation that is designed to protect consumers by establishing national standards for data security and notification. We applaud the work of this Committee and, especially, the cosponsors of H.R. 3997, for their attention to our views throughout the preparation of this legislation. The approach taken by H.R. 3997 to the issue of data security and breach notification is, we believe, consistent with the kind of narrowly tailored, targeted legislation that we believe ought to be the objective of Congressional action in this area. A broader bill, one that incorporates non-germane and unrelated subjects into the data security debate, will inevitably distract from the goal of responding to the absence of federal law that we and our members believe needs to occur sooner rather than later.

As the Chairman and the Subcommittee know, the issues of data security and notification are unusual in that very similar bills have been and are currently under consideration by no less than six Congressional Committees. In the Senate, the Senate Commerce Committee has already reported its bill, S. 1408, and the Senate Judiciary Committee responded by reporting S. 1326, a bill introduced by Senator Jeff Sessions (R-AL). The Senate Banking Committee has held hearings, the most recent of which took place on September 22, and has also promised legislative action. Moreover, due to the inclusion of unrelated matters in S. 1408, such as restrictions on the sale and use of social security numbers, along with language mandating credit freezes, Senate Finance Chairman Charles Grassley (R-IA) has publicly expressed an interest in examining at least the social security component of S. 1408.

In the House, this Committee was the first to act, introducing an earlier version of this legislation, H.R. 3375. The House Commerce Committee has followed with the recent introduction H.R. 4127, reporting it out of Subcommittee last week. Finally, the House Judiciary Committee, like its Senate counterpart, has expressed an interest in acting on this subject as well.

Principles to be Employed in Federal Data Security Legislation

The Coalition recognizes that having so many Congressional Committees engaged in this debate represents a public recognition that the series of data breaches that have taken place during the past year has threatened the confidence that consumers have in businesses that have custody of sensitive personal information pertaining to them. We believe that there is therefore a pressing need for Congress to address deficiencies in the law that currently fail to adequately regulate the interstate application of uniform national standards for data security and, in the event of a

breach of that security, the timely notification of a breach to consumers so they can protect themselves from the potential risk of identity theft. It is not in the interest of the public to expand the impact of such legislation into unrelated and more controversial subjects.

In the course of our deliberations, we have identified a series of principles which we believe ought to be incorporated into any legislation this area that the Congress ultimately enacts.

1. **Preemption.** Starting with the passage, in 2003, of California's data breach and notification legislation (SB 1386, codified as sec. 1798.29 and 1798.82 of the California Civil Code), twenty-one other states – and one municipality – have adopted variations on that original theme. But they are far from alike. New Jersey's new law (A. 4001), like California's, has a fairly low breach notification trigger, and other states vary on how they define the operative terms of their respective statutes. These terms include "personal information", what constitutes a "security breach", and the conditions which would give rise to a mandatory obligation to provide notice of a breach, such as "unauthorized acquisition" of data, or "acquisition" that creates a "risk of identity theft". States have also differed in their treatment of the scope of data containing sensitive personal information and whether it pertains only to electronic data or paper data, whether the applicable data is computerized, unencrypted or encrypted, or redacted or unredacted. For example, New York State's new law covers computerized data pertaining to personal information, including encrypted data if the encryption key has also been acquired. But the New York City ordinance goes even further, expanding the scope of covered information to include unique biometric data as well as electronic signatures, paper as well as computerized data, whether encrypted or not. In North Carolina, the new law would cover data containing "personal information in any form (whether computerized, paper, or otherwise)", which raises the possibility, by use of the word "otherwise", that even oral statements containing personal information may be subject to regulation under the same law.

Our members are all companies servicing a national and often international clientele. The prospect of an ever-changing patchwork of inconsistent state laws can only have one public policy consequence, and that is to confuse and discourage the use by consumers of the Internet and e-commerce generally. Since there are also more than 100,000 municipalities potentially eligible to follow New York City as a participant in this public policy debate, it should be clear why we believe Congress needs to enact a federal, preemptive statute that provides for the uniform application of national standards.

That said, we are aware that some interests, including, among others, the National Association of Attorneys General ("NAAG"), differ with this position, preferring a state by state approach and arguing that states are and should be allowed to remain "laboratories" in which laws pertaining to data breach and security should

be tested. We obviously disagree and suggest that the objectivity of some of these critics may be compromised by their own interest in preserving their jurisdictional turf. To us, it seems self-evident that nothing is more interstate in nature – and therefore within the Constitutional province of the Congress to act – than the computerized transmission of data. Even a federal floor for law in this area, advocated by some, would have no practical effect other than merely to create a different sort of "patchwork" of ever-shifting compliance obligations. Online and offline commerce alike would inevitably suffer from either a federal floor, which states – and localities, for that matter – could exceed, or, as the NAAG and others propose, the simple addition of a federal standard to the potential of 50 different state standards. For businesses such as our members, a regulatory regime like this would be a compliance nightmare, a game of regulatory "gotcha", with consumers in different states subject to different protections, depending exclusively on where, by chance, they happen to live.

We therefore applaud the preemptive provisions of H.R. 3997. They seek to recognize the critical national importance of consistent enforcement and reliable consumer expectations, as well as the reality that a federal bill without meaningful preemption is of little public policy value and only serves to further complicate the enforcement landscape that companies like those we represent have to face.

2. **National Security Standard.** In 1999, the Congress concluded a decade of debate with the historic enactment of the Gramm-Leach-Bliley Act ("GLB"). In section 501(b) of GLB, "financial institutions" were specifically required to implement appropriate "administrative, technical, and physical safeguards" designed to protect the security and integrity of personal information pertaining to their customers. The regulations that followed recognized and underscored that obligation, and it was based on GLB's requirements that some states began to expand a similar obligation to non-financial institutions. Our membership, as we noted earlier, is a diverse one, and just as we have among our members financial institutions such as Charles Schwab & Co., CIGNA, Fidelity Investments, Assurant, CheckFree, JPMorgan Chase, American Century Investments and MasterCard, we also have, as members, non-financial companies such as The Procter & Gamble Company and Eastman Kodak. We also recognize that, in the wake of GLB, a growing number of companies, best known, perhaps, as non-financial companies, also have as part of their corporate structure financial components that are already subject to GLB-based regulation. Examples of such hybrid obligations among our members include Deere & Co., General Electric Company and General Motors.

The Coalition therefore supports legislation, such as HR 3997, that expands, nationwide, the obligation to provide for the security of personal data to include non-financial institutions as well as financial institutions. We believe that the obligation to provide satisfactory security should not generate an industry specific solution but, rather, follow the data, with an appreciation for the differences in business models.

There are, of course, variations in the capacity of different businesses to provide appropriate security for sensitive personal data, and we recommend that, like functional regulators in the case of financial institutions, the Federal Trade Commission ("FTC") is the appropriate regulator to assure that non-financial companies provide security that is "similar to" that which financial institutions are obligated to provide and appropriate for their size and capacity.

H.R. 3997 fulfills this obligation, and establishes an affirmative obligation on all businesses to provide "reasonable policies and procedures to protect the security and confidentiality" of sensitive personal information pertaining to consumers.

3. **Reasonable Notification Trigger.** When GLB was enacted, section 502(b) obligated financial institutions to provide notices to consumers that were designed to inform them that they had the right to "opt out" of allowing companies to share "nonpublic personal information" pertaining to them with third parties. In its review of the effectiveness of this notice requirement, following enactment of GLB, the FTC found that 98% of recipients failed to read the notices, much less act upon them. In the course of the development of this legislation, Congress therefore has the unusual benefit of hindsight, and we therefore know, in advance, that notifications that are not tied to an actual, actionable threat to the consumer are probably destined, like all but 2% of the GLB privacy notices, to be discarded with the weekly trash. We therefore believe the California style notification standard of "unauthorized acquisition" is far too low and will lead, inevitably, to over-notification, which, in turn, defeats the underlying purpose of a notification regime. In that context, it is worth noting that since July 1, 2003, when the California statute became effective, the California Office of Privacy Protection ("OPP") has tracked 83 reported breaches in that state, from a wide range of sources. As of February of this year, Joanne McNabb, the chief of OPP, reportedly was unable to link more than one of what were then 45 breaches to an instance of identity theft related to one of the consumers about whom the breached information applied. However, Ms. McNabb has since stopped trying to apply a link to any of the subsequent 38 breaches that have been reported in California.

It is equally important, though, to remember that companies are always free to unilaterally provide notices whenever they believe it is appropriate to do so, and market competition in this area always plays a dominant role, especially for companies, like members of the Coalition, who view themselves as responsible custodians of personally sensitive information pertaining to their customers. That said, it is an altogether different matter for the federal government to establish a mandate for custodians of sensitive personal information that will inevitably result in a notification regime unrelated to harm or any significant threat of harm. We are aware that some policymakers prefer notice any time a breach occurs, notwithstanding its likely impact on consumers. We believe this approach is unwise and, if embraced, will likely defeat the express purpose of a notification regime by

over-notifying consumers in such a way that we know, by virtue of the GLB privacy notice example, that they will very likely discard those notices to their disadvantage. As FTC Commissioner Leary noted in his testimony before the Senate Commerce Committee on June 16, 2005, such a legislative imperative would likely create a result akin to that which occurs in Aesop's well-known fable, "The Boy Who Cried Wolf."

Earlier this year, the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision ("OTS"), the Office of the Comptroller of the Currency ("OCC"), and the Board of Governors of the Federal Reserve System ("FED") issued interagency guidelines ("Interagency Guidance"), pursuant to authority granted by GLB, that proposed that notices be issued whenever it is reasonable to expect that sensitize personal information will be "misused" in an manner that creates "substantial harm or inconvenience" to the consumer. We believe it is essential for Congress to articulate the broad parameters of what regulators should consider when providing guidance to the industries under their supervision, and we would prefer that that standard parallel the one endorsed by FTC Chairwoman Deborah Majoras in testimony she delivered last June before the Senate Commerce Committee. She suggested a standard for notification that ties a breach to a "significant risk of identity theft". As she observed when she testified, "It is important to note...that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." We would add that they can also happen – and be caught by the victim of the breach – before any risk of any kind affects consumers.

The Coalition recognizes that HR 3997 has embraced language tracking the OCC guidance as the trigger for notification, but it has also performed a public service by trying to define the term in section 630(k)(11) in the way it has. We also hope that the Securities and Exchange Commission ("SEC"), like the Interagency Guidance, will act as soon as practicable to follow the example of the other functional regulators and provide interim guidance for businesses that they supervise.

4. **Reasonable Compliance Obligation.** Breach security and notification are complicated matters, and how security is defined and implemented is equally technical. We believe that the functional regulators of the affected industries, including the FTC for those businesses not currently subject to functional regulation, are best suited to supervise and enforce the decisions Congress makes in this arena. Only they can adequately evaluate the risks to consumers served by the whole range of businesses that have custody over sensitive personal information pertaining to them. Only they can adequate track evolving technology, and adjust quickly and over time to effectively translate changes in that environment into regulations that are both reasonable and consistent with the law enacted by the Congress. Our members applaud the language in H.R. 3997, in proposed new section 630(i) of the FCRA, that attempts to encourage functional regulators to "jointly" develop regulations and to reconcile any differences by a date certain. The decision the bill makes, in proposed

subsection (j), to delegate exclusive enforcement authority to functional regulators is, in our judgment, a wise and prudent decision.

Conclusion

In summary, the National Business Coalition on E-Commerce and Privacy supports the House Financial Services Committee's approach to this very important problem, as embodied in the legislative language of H.R. 3997. As we have said from the inception of this debate, it is critical to approach the problem of data security and notification in a responsible and thoughtful manner, keeping in mind the need to narrowly tailor legislation that embraces the principles which the Coalition has articulated above. We are pleased that most of the bills now under consideration have been drafted, to one degree or another, with these principles in mind.

As we have also tried to demonstrate in this statement, it is equally important that during the course of its consideration of H.R. 3997, the Committee resist the temptation to expand the coverage of this legislation to include subjects unrelated to data security and notification, such as efforts to require (for privacy reasons) consumer rights to access and correct data held by businesses, regardless of any breach of security. As H.R. 3997 evidences, the issues of data security and breach notification involve the security of sensitive personal information from unauthorized access by illegal activity or negligent behavior, while data privacy involves the regulation of lawful sharing of such data by businesses that legally acquire and safeguard it. The two issues should be addressed separately, as acknowledged by the current framework of H.R. 3997.

On behalf of the Coalition, we look forward to the opportunity to continue to work with the Members of this Subcommittee and the full Committee, and their staffs, as this legislative process proceeds.

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
750 FIRST STREET NE SUITE 1100
WASHINGTON, D.C. 20002
(202) 326-6018
(202) 408-6998
http://www.naag.org

LYNNE M. ROSS
Executive Director

PRESIDENT
STEPHEN CARTER
Attorney General of Indiana

PRESIDENT-ELECT
THURBERT BAKER
Attorney General of Georgia

VICE PRESIDENT
LAWRENCE WASDEN
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

October 27, 2005

Honorable Bill Frist
Senate Majority Leader
509 Senate Hart Office Building
Washington, D.C. 20510-4205

Honorable Harry M. Reid
Senate Minority Leader
528 Senate Hart Office Building
Washington, D.C. 20510-3903

Honorable J. Dennis Hastert
Speaker of the House
235 Cannon House Office Building
Washington, D.C. 20515-1314

Honorable Nancy Pelosi
House Minority Leader
2371 Rayburn House Office Building
Washington, D.C. 20515-0508

Dear Congressional Leaders:

We, the undersigned Attorneys General, applaud the efforts of your committee and others to consider enactment of a national security breach notification and security freeze law. Over the past year, the public has become aware of numerous incidences of security breaches, exposing millions of consumers to harm, including potential identity theft, a serious and rapidly growing crime that now costs our nation over $50 billion per year. The issues under consideration by your committee could provide critical assistance to identity theft victims in our states and throughout the nation.

To assist your efforts, we offer the following comments, representing our views on certain critical issues relating to your consideration of security breach notification and security freeze legislation.

1. **Enact a strong security breach notification law**

We call on Congress to enact a national security breach notification law that will provide meaningful information to consumers. If Congress is not able to enact a strong notice law, it should leave the issue to state law, which is responding strongly. Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by theft of personal information. The Federal Trade Commission (FTC) reports that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly. For example, when the misuse was discovered within five months of its onset, the value of the damage was less than $5,000 in 82% of the cases. When victims did not discover the misuse for six months or more, the value of the damage was $5,000 or more in 44% of the cases. In addition, new accounts were opened in fewer than 10% of the cases when it took victims less than a month to discover that their information was being misused, while new accounts were opened in 45% of cases when six months or more elapsed before the misuse was discovered.

The public has become aware of the numerous incidences of security breaches over the past year as a result of California's security breach notification laws, which went into effect on July 1, 2003. These laws require businesses and California public institutions to notify the public about any breach of the security of their computer information system where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The public has become so concerned about security breaches and their potential role in the increased incidence of identity theft that 21 additional states have enacted

security breach notification laws over the past year: Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington.

We urge your committee to enact a meaningful federal security breach notification provision that is at least as protective of consumers as California law. A meaningful federal security breach notification law would, in our view, broadly define what constitutes a security breach and the notice requirements in order to give consumers a greater level of protection. For example, "security breach" should be broadly defined as "unauthorized acquisition of or access to computerized or other data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." We also believe that the standard for notification should be tied to whether personal information, whether in electronic or paper form, was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud. It is certain, however, that creating an additional trigger requirement relating to proof of risk will result in fewer notices than consumers now receive under many state laws. We note that the majority of states that have enacted security breach notification laws – California, Georgia, Illinois, Indiana, Maine, Minnesota, Nevada, New York, North Dakota, Ohio, Rhode Island, Tennessee,

and Texas – do not require any additional trigger requirement before notice about a breach is required to be given to affected consumers.

In the event that Congress decides to consider the concept of harm in addition to the unauthorized acquisition of personal information in the context of security breach notification, we urge Congress to cast this element as an exception, not a trigger, in order to make it plain that notice must be given in the absence of sufficient information. Such an exception could contain the following provisions: (1) security breach notices must be provided to consumers unless there is "no risk of harm or misuse of personal information" – not "no risk of identity theft" – resulting from the breach; (2) security breach notices must be provided to consumers in the event that it cannot be determined whether or not there will be a risk of harm or misuse of personal information; (3) the breached entity should be required to consult with law enforcement and receive an affirmative written response with respect to the determination that there is no risk of harm resulting from the breach; and (4) any determination by law enforcement that there is "no risk of harm or misuse of personal information" should be made in writing and filed with both the FTC and with the State Attorney General from the state in which the breach occurred.

In addition to an acquisition-based notification standard, we believe that an effective federal security breach notification law should have the following additional provisions:

- Coverage of all entities, including financial institutions governed by the Gramm-Leach-Bliley Act. Financial institutions, which may hold very sensitive data

about consumers, should not be subject to a lesser standard for giving notice under their regulatory guidelines than other entities are held to by statute.

- Inclusion of the following as "personal information" that, if acquired or accessed by an unauthorized person, would trigger notification: an individual's first name or first initial and last name, or the name of a business, in combination with any one or more of the following data elements, when either the name or the data element is not encrypted:
    - Social Security number.
    - Driver's license number or government-issued identification number.
    - Account number, credit or debit card number, alone or in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    - A unique electronic identification number, email address, or routing code alone or in combination with any required security code, access code, or password.
    - Unique biometric data such as fingerprint, voice print, a retina or iris image, or other unique physical representation.
    - Home address or telephone number.
    - Mother's maiden name.
    - Month and year of birth.
    - Such other information as the FTC may add by regulation.
- Notification provisions that would, at a minimum, provide the following notices to consumers: individual notice by mail or by email if the consumer has

consented to email in a manner consistent with the requirements of the Electronic Signatures in Global and National Commerce Act; substitute notice, if permitted at all, could be an option only when more than 500,000 consumers are affected and should require publication on a website and in major statewide or national news media.

- No "fraud monitoring" exemptions, especially when the compromised information relates to a debit card, bank account, or other non-credit account.

2. **Enact a strong federal security freeze law.**

We also call on Congress to enact a strong federal security freeze law. The 2003 amendments to the federal Fair Credit Reporting Act gave consumers the right to place a "fraud alert" on their credit reports for at least 90 days, with extended alerts lasting for up to seven years in cases where identity theft occurs. Several states have enacted stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches. Five states – California, Louisiana, Texas, Vermont, and Washington – already allow consumers to place a "security freeze" on their credit report. A security freeze allows a consumer to control who will receive a copy of his or her credit report, thus making it nearly impossible for criminals to use stolen information to open an account in the consumer's name. Security freeze provisions will become effective in the next several months in the following additional seven states: Colorado, Connecticut, Illinois, Maine, Nevada, New Jersey, and North Carolina.

We believe that security freeze laws that give all consumers the right to use a freeze as a prevention tool are one of the most effective tools available to stop the harm that can result from data heists. If Congress is inclined to create a federal security freeze

law, we urge Congress to make such a law meaningful by modeling it on the best provisions in comparable state laws, including:

- Creating a security freeze that is available to all consumers at no fee or a low-capped fee.
- Banning fees for victims of identity theft who have a police report or FTC affidavit, seniors, veterans, and persons who receive a notice of security breach.
- Allowing consumers who choose to implement a freeze to also have the ability to selectively or temporarily lift the freeze, again at no charge to victims of identity theft, seniors, veterans, and persons who receive a notice of security breach, and to other consumers at a modest, capped fee.
- Ensuring that the security freeze provisions apply to all entities who may examine a credit file in connection with new accounts, including accounts for goods and services, such as cell phones, utilities, rental agreements, and the like.
- Allowing consumers who choose to implement a freeze with all three major national consumer reporting agencies to be able to do so by contacting one of them, rather than all three individually.

3. Allow the State Attorneys General to enforce the new federal security breach notification and security freeze laws in state or federal court.

We further call on Congress to ensure that State Attorneys General can enforce any new federal security breach notification and security freeze laws. The FTC continues to do a commendable job in enforcing its current laws, including the FTC Act and the

Gramm-Leach-Bliley Act, against entities that have not employed sufficient protections to safeguard consumers' personal information. However, consumers would suffer if Congress were to make the FTC the sole enforcer of new laws requiring security breach notification and security freezes. Indeed, State Attorneys General are currently involved in investigating security breaches and enforcing available state standards relating to use of adequate procedures and processes to protect consumers' personal information. Congress should ensure that State Attorneys General continue to play their important role in protecting consumers from practices that could lead to identity theft.

4. Do not preempt the power of states to enact and enforce state security breach notification and security freeze laws.

We urge Congress to not preempt the states in these two important consumer protection areas, or indeed in other areas. Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.

In the event that Congress determines that it will consider preemption of the states in these areas, we urge Congress at a minimum to narrowly tailor preemption so that only those states laws that are "inconsistent" with the federal laws would be preempted, and then "only to the extent of the inconsistency." This is important because Congress may enact a security breach notification law or a security freeze law that does not cover all entities, and the states should be allowed to enact laws that cover those additional entities. While we oppose preemption in general, it is particularly important that if Congress does

adopt some degree of preemption, that preemption be limited to the timing, manner, and content of notices of security breach, and not interfere with other state laws addressing the subject of, or consequences of, a security breach.

Thank you for considering our recommendations. We look forward to working with you on this important legislation in the coming weeks and months.

Sincerely,

David W. Márquez
Attorney General of Alaska

Terry Goddard
Attorney General of Arizona

Mike Beebe
Attorney General of Arkansas

Bill Lockyer
Attorney General of California

John Suthers
Attorney General of Colorado

Richard Blumenthal
Attorney General of Connecticut

M. Jane Brady
Attorney General of Delaware

Robert J. Spagnoletti
Attorney General of District of Columbia

Thurbert E. Baker
Attorney General of Georgia

Mark J. Bennett
Attorney General of Hawaii

Stephen H. Levins, Executive Director
Hawaii Ofc. Consumer Protection

Lawrence G. Wasden
Attorney General of Idaho

Lisa Madigan
Attorney General of Illinois

Gregory D. Stumbo
Attorney General of Kentucky

G. Steven Rowe
Attorney General of Maine

Tom Reilly
Attorney General of Massachusetts

Mike Hatch
Attorney General of Minnesota

Jay Nixon
Attorney General of Missouri

Jon Bruning
Attorney General of Nebraska

Kelly Ayotte
Attorney General of New Hampshire

Eliot Spitzer
Attorney General of New York

Tom Miller
Attorney General of Iowa

Charles Foti
Attorney General of Louisiana

J. Joseph Curran, Jr.
Attorney General of Maryland

Mike Cox
Attorney General of Michigan

Jim Hood
Attorney General of Mississippi

Mike McGrath
Attorney General of Montana

Brian Sandoval
Attorney General of Nevada

Peter C. Harvey
Attorney General of New Jersey

Roy Cooper
Attorney General of North Carolina

Wayne Stenehjem
Attorney General of North Dakota

Jim Petro
Attorney General of Ohio

Hardy Myers
Attorney General of Oregon

Roberto J. Sanchez-Ramos
Attorney General of Puerto Rico

Henry McMaster
Attorney General of South Carolina

Paul G. Summers
Attorney General of Tennessee

Mark Shurtleff
Attorney General of Utah

Rob McKenna
Attorney General of Washington

Pamela Brown
Attorney General of Northern Mariana Islands

W.A. Drew Edmondson
Attorney General of Oklahoma

Tom Corbett
Attorney General of Pennsylvania

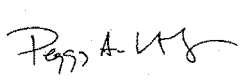
Patrick Lynch
Attorney General of Rhode Island

Larry Long
Attorney General of South Dakota

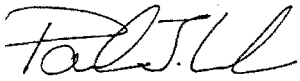
Greg Abbott
Attorney General of Texas

William H. Sorrell
Attorney General of Vermont

Darrell V. McGraw, Jr.
Attorney General of West Virginia



Peggy A. Lautenschlager
Attorney General of Wisconsin



Patrick J. Crank
Attorney General of Wyoming

cc: Chairman Shelby & Ranking Member Sarbanes
Senate Committee on Banking, Housing, and Urban Affairs

Chairman Stevens & Ranking Member Inouye
Senate Committee on Commerce, Science, & Transportation

Chairman Specter & Ranking Member Leahy
Senate Committee on the Judiciary

Chairman Barton & Ranking Member Dingell
House Committee on Energy & Commerce

Chairman Oxley & Ranking Member Frank
House Committee on Financial Services

Chairman Sensenbrenner & Ranking Member Conyers
House Committee on the Judiciary

1. Of the states listed, Hawaii is also represented by its Office of Consumer Protection, an agency which is not a part of the state Attorney General's Office, but which is statutorily authorized to represent the State of Hawaii in consumer protection actions. For the sake of simplicity, the entire group will be referred to as the "Attorneys General," and such designation as it pertains to Hawaii, refers to the Attorney General and Executive Director of the State of Hawaii Office of Consumer Protection.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

EXECUTIVE HEADQUARTERS
2301 McGee Street
Suite 800
Kansas City MO
64108-2662
voice 816-842-3600
fax 816-783-8175

FEDERAL AND INTERNATIONAL RELATIONS
Hall of the States
444 North Capitol St NW
Suite 701
Washington DC
20001-1509
voice 202-624-7790
fax 202-624-8579

SECURITIES VALUATION OFFICE
48 Wall Street
6th Floor
New York NY
10005-2906
voice 212-398-9000
fax 212-382-4207

WORLD WIDE WEB
www.naic.org

November 8, 2005

Honorable Spencer Bachus
Chairman
Honorable Bernard Sanders
Ranking Minority Member
Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

SUBJECT: Financial Data Protection Act of 2005 – HR 3997

Dear Chairman Bachus and Ranking Member Sanders:

On behalf of state insurance regulators, the National Association of Insurance Commissioners (NAIC) would like to offer the following comments for consideration by the Subcommittee on Financial Institutions and Consumer Credit regarding HR 3997, the "Financial Data Protection Act of 2005".

HR 3997 would amend the Fair Credit Reporting Act (FCRA) by adding a new Section 630, entitled "Data Security Safeguards", establishing specific federal data security requirements for most entities in the United States, including insurance companies and producers already regulated by the states under the McCarran-Ferguson Act and the Gramm-Leach-Bliley Act (GLBA). The true strength of the state regulatory system in protecting consumers at the local level in the communities where they live was recognized by Congress in these primary federal laws dealing with proper supervision of the business of insurance. Under the McCarran-Ferguson Act and GLBA, states are permitted to establish higher consumer protection standards than those mandated by federal law, and many states have chosen to do so. HR 3997 seeks an opposite result by imposing a federal ceiling on the authority of states to protect their consumers on privacy and data security matters.

State insurance regulators and the NAIC enthusiastically support strong laws and regulations protecting the privacy of individual consumer information. Every state has adopted comprehensive privacy laws to protect the extensive personal information collected by insurers to underwrite and administer insurance policies. The primacy and importance of these state privacy laws were specifically recognized and embraced by Congress in Title V of GLBA. Insurance regulators also support efforts by our state and federal legislators to mandate fair treatment and notification to consumers when their private information is improperly disclosed to third parties, especially where such unauthorized disclosures might result in identity theft.

HR 3997 provides that "any person" operating in interstate commerce who is engaged in assembling or evaluating "information on consumers" must implement and maintain reasonable policies and procedures to protect the security and confidentiality of "sensitive financial personal information". Under FCRA (which HR 3997 would amend), "person" is defined to mean any individual, business, government, or other entity. Consequently, the "persons" subject to the mandates of HR 3997 would encompass almost every business, government, or individual entity in the United States that collects health, financial, or other information on consumers. Such persons would be required to investigate possible breaches of data security and provide notices and certain remedies to affected consumers.

While state regulators applaud the goal of safeguarding sensitive personal financial data, we are deeply concerned that several sweeping provisions in HR 3997 go far beyond that goal and would seriously weaken privacy protections for consumers. HR 3997 seeks to preempt all state privacy laws protecting consumer health, lifestyle, and financial data collected by insurers to underwrite and administer insurance policies, even though such information is not used in commercial transactions that lead to identify theft. <u>If state laws are preempted, consumers will not receive the privacy safeguards promised to them in GLBA regarding personal financial and health information collected by insurance companies.</u>

H.R. 3997 has several troubling provisions that would undermine or negate the efforts of state insurance regulators to enforce fair market conduct and protect the security and confidentiality of consumer information that is collected, maintained, transferred, and used by insurance companies. State insurance departments also offer cost-free assistance to consumers to intercede with insurers and help negotiate fair solutions when problems occur. These could also be undermined.

- First, the blanket federal preemption of state laws in HR 3997 far exceeds the purpose and scope of the bill itself, which is to prevent and mitigate identity theft. Although HR 3997 is aimed at protecting sensitive personal information used in financial transactions, the vast scope of its federal preemption provision would effectively prohibit a state from protecting ANY type of consumer information, including health and medical information, lifestyle and income information, claims history information, and employment information, to name a few.

- Second, HR 3997 would change the existing operation of FCRA by expanding its reach to encompass far more than consumer reporting agencies and persons that use consumer reports for credit and employment purposes. At present, FCRA is a law with a narrow purpose of promoting national credit markets, and its federal preemption provision is limited solely to state laws that conflict with its narrow purpose. HR 3997 adds new and different definitions and provisions to FCRA that greatly expand its scope to cover data security requirements in all industries. These additional terms and changes to the mission of FCRA involve numerous subjective judgments that could confuse and complicate decision-making by business and government entities that use FCRA.

- Third, HR 3997 appears to rewrite the powers and responsibilities of states as regulators already set forth in GLBA by taking away their authority to develop and implement privacy and data security regulations. Title V of GLBA expressly recognizes exclusive state authority to establish privacy and data security requirements that exceed federal minimum requirements. Similarly, HR 3997 appears to conflict with other federal laws that depend on states to accomplish federal goals, such as the Health Insurance Portability and Accountability Act.

- Fourth, HR 3997 does not provide the same high level of consumer protection that is found in many state privacy and data security laws. Several states have laws that provide "opt-in" privacy rights and immediate notification of data security breaches with no restrictions on the right of consumers or a state attorney general to seek damages from companies that abuse personal information. Insurance markets will not work if consumers believe that their highly personal information submitted to insurers is inadequately protected by state laws and enforcement actions.

- Fifth, HR 3997 undercuts the authority of individual states to protect their own residents when a data security breach happens. The bill assigns enforcement of its federal data security requirements to an insurer's state of domicile, which may be far removed from the location of consumers who are harmed by a breach of data security or weak safeguards. The strength of state consumer protection efforts is to ensure that local officials have authority to monitor an insurer's conduct and take enforcement actions to prevent harm to local residents.

In short, HR 3997 would take away existing state consumer privacy laws, market conduct enforcement authority, and data security safeguards for the purpose of establishing a federal system that limits consumer protection to being notified under certain circumstances when a breach of data security occurs. The NAIC believes that restricting the scope of the bill to personally-identifiable financial information and implementing safeguards through state authority under GLBA would achieve the benefits sought by Congressional sponsors, while avoiding unnecessary harm to the consumer protection

authority of state insurance regulators regarding privacy and other important insurance matters.

Thank you for considering the views of NAIC. We look forward to assisting the House Financial Services Committee and other Members of Congress as you develop data security legislation that would effectively protect consumers without surrendering their other essential rights under state and federal law.

Sincerely,

Diane Koken
Commissioner of Insurance, Pennsylvania
President, NAIC

BUSINESS & COMMERCE CODE

CHAPTER 20. REGULATION OF CONSUMER CREDIT REPORTING AGENCIES

Sec. 20.01. DEFINITIONS. In this chapter:

(1) "Adverse action" includes:

(A) the denial of, increase in a charge for, or reduction in the amount of insurance for personal, family, or household purposes;

(B) the denial of employment or other decision made for employment purposes that adversely affects a current or prospective employee; or

(C) an action or determination with respect to a consumer's application for credit that is adverse to the consumer's interests.

(2) "Consumer" means an individual who resides in this state.

(3) "Consumer file" means all of the information about a consumer that is recorded and retained by a consumer reporting agency regardless of how the information is stored.

(4) "Consumer report" means a communication or other information by a consumer reporting agency relating to the credit worthiness, credit standing, credit capacity, debts, character, general reputation, personal characteristics, or mode of living of a consumer that is used or expected to be used or collected, wholly or partly, as a factor in establishing the consumer's eligibility for credit or insurance for personal, family, or household purposes, employment purposes, or other purpose authorized under Sections 603 and 604 of the Fair Credit Reporting Act (15 U.S.C. Sections 1681a and 1681b), as amended. The term does not include:

(A) a report containing information solely on a transaction between the consumer and the person making the report;

(B) an authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;

(C) a report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer makes a decision with respect to the request, if the third party advises the consumer of the name

and address of the person to whom the request was made and the person makes the disclosures that must be made under Section 615 of the Fair Credit Reporting Act (15 U.S.C. Section 1681m), as amended, to the consumer in the event of adverse action against the consumer;

(D) any communication of information described in this subdivision among persons related by common ownership or affiliated by corporate control; or

(E) any communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity before the time that the information is initially communicated to direct that such information not be communicated among such persons.

(5) "Consumer reporting agency" means a person that regularly engages wholly or partly in the practice of assembling or evaluating consumer credit information or other information on consumers to furnish consumer reports to third parties for monetary fees, for dues, or on a cooperative nonprofit basis. The term does not include a business entity that provides only check verification or check guarantee services.

(6) "Investigative consumer report" means all or part of a consumer report in which information on the character, general reputation, personal characteristics, or mode of living of a consumer is obtained through a personal interview with a neighbor, friend, or associate of the consumer or others with whom the consumer is acquainted or who may have knowledge concerning any such information. The term does not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when the information was obtained directly from a creditor of the consumer or from the consumer.

(7) "Security alert" means a notice placed on a consumer file that alerts a recipient of a consumer report involving that consumer file that the consumer's identity may have been used without the consumer's consent to fraudulently obtain

goods or services in the consumer's name.

(8) "Security freeze" means a notice placed on a consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file without the express authorization of the consumer.

Added by Acts 1997, 75th Leg., ch. 1396, Sec. 33(a), eff. Oct. 1, 1997. Amended by Acts 2003, 78th Leg., ch. 1326, Sec. 1, eff. Sept. 1, 2003.

Sec. 20.02. PERMISSIBLE PURPOSES; PROHIBITION; USE OF CONSUMER'S SOCIAL SECURITY NUMBER. (a) A consumer reporting agency may furnish a consumer report only:

(1) in response to a court order issued by a court with proper jurisdiction;

(2) in accordance with the written instructions of the consumer to whom the report relates; or

(3) to a person the agency has reason to believe:

(A) intends to use the information in connection with a transaction involving the extension of credit to, or review or collection of an account of, the consumer to whom the report relates;

(B) intends to use the information for employment purposes as authorized under the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.), as amended, and regulations adopted under that Act;

(C) intends to use the information in connection with the underwriting of insurance involving the consumer as authorized under the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.), as amended, and regulations adopted under that Act;

(D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental entity required by law to consider an applicant's financial responsibility or status;

(E) has a legitimate business need for the information in connection with a business transaction involving the consumer; or

(F) intends to use the information for any

Bill Number: TX79RSB 122 Date: 05-28-2005

ENROLLED

AN ACT

relating to the prevention and punishment of identity theft and the rights of certain victims of identity theft; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. (a) Chapter 2, Code of Criminal Procedure, is amended by adding Article 2.29 to read as follows:

Art. 2.29. REPORT REQUIRED IN CONNECTION WITH FRAUDULENT USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) A peace officer to whom an alleged violation of Section 32.51, Penal Code, is reported shall make a written report to the law enforcement agency that employs the peace officer that includes the following information:

(1) the name of the victim;

(2) the name of the suspect, if known;

(3) the type of identifying information obtained, possessed, transferred, or used in violation of Section 32.51, Penal Code; and

(4) the results of any investigation.

(b) On the victim's request, the law enforcement agency shall provide the report created under Subsection (a) to the victim. In providing the report, the law enforcement agency shall redact any otherwise confidential information that is included in the report, other than the information described by Subsection (a).

(b) The change in law made by this section applies only to

the investigation of an offense committed on or after September 1, 2005. The investigation of an offense committed before September 1, 2005, is covered by the law in effect when the offense was committed, and the former law is continued in effect for that purpose. For purposes of this subsection, an offense is committed before September 1, 2005, if any element of the offense occurs before that date.

SECTION 2. Title 4, Business & Commerce Code, is amended by adding Chapter 48 to read as follows:

CHAPTER 48. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 48.001. SHORT TITLE. This chapter may be cited as the Identity Theft Enforcement and Protection Act.

Sec. 48.002. DEFINITIONS. In this chapter:

(1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device.

(2) "Sensitive personal information":

(A) means an individual's first name or first

initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

(B) does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

(3) "Telecommunication access device" has the meaning assigned by Section 32.51, Penal Code.

(4) "Victim" means a person whose identifying information is used by an unauthorized person.

(Sections 48.003-48.100 reserved for expansion)

SUBCHAPTER B. IDENTITY THEFT

Sec. 48.101. UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION. (a) A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

(b) It is a defense to an action brought under this section that an act by a person:

(1) is covered by the Fair Credit Reporting Act (15

U.S.C. Section 1681 et seq.); and

(2) is in compliance with that Act and regulations adopted under that Act.

(c) This section does not apply to:

(1) a financial institution as defined by 15 U.S.C. Section 6809; or

(2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

Sec. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

Sec. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF

1 SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of
2 system security" means unauthorized acquisition of computerized
3 data that compromises the security, confidentiality, or integrity
4 of sensitive personal information maintained by a person. Good
5 faith acquisition of sensitive personal information by an employee
6 or agent of the person or business for the purposes of the person is
7 not a breach of system security unless the sensitive personal
8 information is used or disclosed by the person in an unauthorized
9 manner.
10 (b) A person that conducts business in this state and owns
11 or licenses computerized data that includes sensitive personal
12 information shall disclose any breach of system security, after
13 discovering or receiving notification of the breach, to any
14 resident of this state whose sensitive personal information was, or
15 is reasonably believed to have been, acquired by an unauthorized
16 person. The disclosure shall be made as quickly as possible, except
17 as provided by Subsection (d) or as necessary to determine the scope
18 of the breach and restore the reasonable integrity of the data
19 system.
20 (c) Any person that maintains computerized data that
21 includes sensitive personal information that the person does not
22 own shall notify the owner or license holder of the information of
23 any breach of system security immediately after discovering the
24 breach, if the sensitive personal information was, or is reasonably
25 believed to have been, acquired by an unauthorized person.
26 (d) A person may delay providing notice as required by
27 Subsections (b) and (c) at the request of a law enforcement agency

that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

(e) A person may give notice as required by Subsections (b) and (c) by providing:

(1) written notice;

(2) electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or

(3) notice as provided by Subsection (f).

(f) If the person or business demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) electronic mail, if the person has an electronic mail address for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one

time more than 10,000 persons of a breach of system security, the person shall also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. Section 1681a, that maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

(Sections 48.104-48.200 reserved for expansion)

SUBCHAPTER C. REMEDIES AND OFFENSES

Sec. 48.201. CIVIL PENALTY; INJUNCTION. (a) A person who violates this chapter is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring suit to recover the civil penalty imposed by this subsection.

(b) If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of this state against the person to restrain the violation by a temporary restraining order or a permanent or temporary injunction.

(c) An action brought under Subsection (b) shall be filed in a district court in Travis County or:

(1) in any county in which the violation occurred; or

(2) in the county in which the victim resides,

regardless of whether the alleged violator has resided, worked, or done business in the county in which the victim resides.

(d) The plaintiff in an action under this section is not required to give a bond. The court may also grant any other equitable relief that the court considers appropriate to prevent

any additional harm to a victim of identity theft or a further violation of this chapter or to satisfy any judgment entered against the defendant, including the issuance of an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets.

(e) The attorney general is entitled to recover reasonable expenses incurred in obtaining injunctive relief, civil penalties, or both, under this section, including reasonable attorney's fees, court costs, and investigatory costs. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter.

(f) The fees associated with an action under this section are the same as in a civil case, but the fees may be assessed only against the defendant.

Sec. 48.202. COURT ORDER TO DECLARE INDIVIDUAL A VICTIM OF IDENTITY THEFT. (a) A person who is injured by a violation of Section 48.101 or who has filed a criminal complaint alleging commission of an offense under Section 32.51, Penal Code, may file an application with a district court for the issuance of a court order declaring that the person is a victim of identity theft. A person may file an application under this section regardless of whether the person is able to identify each person who allegedly transferred or used the person's identifying information in an unlawful manner.

(b) A person is presumed to be a victim of identity theft under this section if the person charged with an offense under

Section 32.51, Penal Code, is convicted of the offense.

(c) After notice and hearing, if the court is satisfied by a preponderance of the evidence that the applicant has been injured by a violation of Section 48.101 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order containing:

(1) a declaration that the person filing the application is a victim of identity theft resulting from a violation of Section 48.101 or an offense under Section 32.51, Penal Code, as appropriate;

(2) any known information identifying the violator or person charged with the offense;

(3) the specific personal identifying information and any related document used to commit the alleged violation or offense; and

(4) information identifying any financial account or transaction affected by the alleged violation or offense, including:

(A) the name of the financial institution in which the account is established or of the merchant involved in the transaction, as appropriate;

(B) any relevant account numbers;

(C) the dollar amount of the account or transaction affected by the alleged violation or offense; and

(D) the date of the alleged violation or offense.

(d) An order rendered under this section must be sealed because of the confidential nature of the information required to

be included in the order. The order may be opened and the order or a copy of the order may be released only:

(1) to the proper officials in a civil proceeding brought by or against the victim arising or resulting from a violation of this chapter, including a proceeding to set aside a judgment obtained against the victim;

(2) to the victim for the purpose of submitting the copy of the order to a governmental entity or private business to:

(A) prove that a financial transaction or account of the victim was directly affected by a violation of this chapter or the commission of an offense under Section 32.51, Penal Code; or

(B) correct any record of the entity or business that contains inaccurate or false information as a result of the violation or offense;

(3) on order of the judge; or

(4) as otherwise required or provided by law.

(e) A court at any time may vacate an order issued under this section if the court finds that the application or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of fact.

(f) A copy of an order provided to a person under Subsection (d)(1) must remain sealed throughout and after the civil proceeding. Information contained in a copy of an order provided to a governmental entity or business under Subsection (d)(2) is confidential and may not be released to another person except as otherwise required or provided by law.

Sec. 48.203. DECEPTIVE TRADE PRACTICE. A violation of

1 Section 48.101 is a deceptive trade practice actionable under
2 Subchapter E, Chapter 17.
3 SECTION 3. This Act takes effect September 1, 2005.
4 _____ _____
5 President of the Senate Speaker of the House
6 I hereby certify that S.B. No. 122 passed the Senate on
7 April 21, 2005, by the following vote: Yeas 31, Nays 0;
8 May 17, 2005, Senate refused to concur in House amendments and
9 requested appointment of Conference Committee; May 20, 2005, House
10 granted request of the Senate; May 26, 2005, Senate adopted
11 Conference Committee Report by the following vote: Yeas 31,
12 Nays 0.
13 _____
14 Secretary of the Senate
15 I hereby certify that S.B. No. 122 passed the House, with
16 amendments, on May 13, 2005, by a non-record vote; May 20, 2005,
17 House granted request of the Senate for appointment of Conference
18 Committee; May 27, 2005, House adopted Conference Committee Report
19 by the following vote: Yeas 142, Nays 0, two present not voting.
20 _____
21 Chief Clerk of the House
22 Approved:
23 _____
24 Date
25 _____
26 Governor