S. HRG. 109–728

EXAMINING THE FINANCIAL SERVICES INDUSTRY'S RESPONSIBILITIES AND ROLE IN PREVENTING IDENTITY THEFT AND PROTECTING SENSITIVE FINANCIAL INFORMATION

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

ON

EXAMINING THE FINANCIAL SERVICES INDUSTRY'S RESPONSIBILITIES AND ROLE IN PREVENTING IDENTITY THEFT AND PROTECTING SENSITIVE FINANCIAL INFORMATION

SEPTEMBER 22, 2005

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

Available at: http://www.access.gpo.gov/congress/senate/senate05sh.html

U.S. GOVERNMENT PRINTING OFFICE

31–069 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

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

RICHARD C. SHELBY, Alabama, *Chairman*

ROBERT F. BENNETT, Utah
WAYNE ALLARD, Colorado
MICHAEL B. ENZI, Wyoming
CHUCK HAGEL, Nebraska
RICK SANTORUM, Pennsylvania
JIM BUNNING, Kentucky
MIKE CRAPO, Idaho
JOHN E. SUNUNU, New Hampshire
ELIZABETH DOLE, North Carolina
MEL MARTINEZ, Florida

PAUL S. SARBANES, Maryland
CHRISTOPHER J. DODD, Connecticut
TIM JOHNSON, South Dakota
JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
EVAN BAYH, Indiana
THOMAS R. CARPER, Delaware
DEBBIE STABENOW, Michigan
ROBERT MENENDEZ, New Jersey

KATHLEEN L. CASEY, *Staff Director and Counsel*
STEVEN B. HARRIS, *Democratic Staff Director and Chief Counsel*
MARK OESTERLE, *Counsel*
SKIP FISCHER, *Senior Staff Professional*
JOHN V. O'HARA *Senior Investigative Counsel*
DEAN V. SHAHINIAN, *Democratic Counsel*
JOSEPH R. KOLINSKI, *Chief Clerk and Computer Systems Administrator*
GEORGE E. WHITTLE, *Editor*

C O N T E N T S

THURSDAY, SEPTEMBER 22, 2005

	Page
Opening statement of Chairman Shelby	1
Opening statements, comments, or prepared statements of:	
Senator Sarbanes	2
Senator Allard	2
Senator Reed	2
Senator Dole	3
Senator Bunning	5
Senator Dodd	22
Senator Carper	30
Senator Pryor	6
Prepared statement	33

WITNESSES

Stuart K. Pratt, President and CEO, Consumer Data Industry Association	8
Prepared statement	34
Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group on Behalf of Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group, and World Privacy Forum	10
Prepared statement	39
Ira D. Hammerman, Senior Vice President and General Counsel, Securities Industry Association	12
Prepared statement	62
Response to written questions of Senator Bunning	74
Gilbert T. Schwartz, Partner, Schwartz & Ballen LLP, on Behalf of the American Council of Life Insurers	13
Prepared statement	66
Response to written questions of Senator Bunning	75
Oliver I. Ireland, Partner, Morrison & Foerster LLP, on Behalf of the American Bankers Association	15
Prepared statement	69
Response to written questions of Senator Bunning	76

EXAMINING THE FINANCIAL SERVICES INDUSTRY'S RESPONSIBILITIES AND ROLE IN PREVENTING IDENTITY THEFT AND PROTECTING SENSITIVE FINANCIAL INFORMATION

THURSDAY, SEPTEMBER 22, 2005

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

The Committee met at 10:25 a.m., in room SD–538, Dirksen Senate Office Building, Senator Richard C. Shelby (Chairman of the Committee) presiding.

OPENING STATEMENT OF CHAIRMAN RICHARD C. SHELBY

Chairman SHELBY. The hearing will come to order. I want to thank my colleague from Arkansas, he is going to join us, Senator Pryor, this morning, but I thought we would move ahead with our opening statements while he is coming.

The broad focus of the hearing this morning, identity theft, is not a subject that is new to this Committee. Indeed, it is far from it. During the Committee's consideration of the Fair Credit Reporting Act, we heard from numerous witnesses who represented various perspectives regarding this issue. Furthermore, we also held additional hearings on this subject independent of the FCRA reauthorization process.

It is important to highlight the Committee's longstanding engagement with respect to this matter. We will spend considerable time and effort attempting to ascertain the nature and the scope of the identity theft threat. As a result, we have directed legal and regulatory changes to provide greater protections for consumers and the overall financial system. Therefore, as we might consider any changes in this area, it is very important that we assess what we are doing in the context of the things we have already done.

That said, I do want to indicate that I am also aware of the fact that the criminal element is constantly searching for new ways to take advantage of consumers and the financial system. In as much, I recognize that this means that we must be constantly vigilant to ensure that we have the means in place to provide the appropriate safeguards necessary relative to the existing threats.

The purpose of today's hearing is to continue this consideration, and we look forward at the proper time to hearing from all of our witnesses.

Senator Sarbanes.

STATEMENT OF SENATOR PAUL S. SARBANES

Senator SARBANES. Thank you very much, Mr. Chairman. I know we are awaiting the arrival of Senator Pryor. Let me first of all comment you for holding the hearing as we examine the question of protecting consumer financial information. You, of course, have been involved in a leadership way on the privacy issue for a number of years, and this Committee does have an important jurisdiction in this area.

I think this is the third hearing we have held in this Congress on this subject. We previously heard from regulators and law enforcement officials, and also from financial institutions and a data broker. We do have these instances occurring where large amounts of information in the hands of private companies go outside the perimeter of security, and of course that raises very serious questions with respect to consumer data breaches.

A number of States have responded to this issue, and have enacted their own legislation, and there are a number of important questions to be addressed, and I welcome this hearing as I welcomed the ones that have preceded it, and I am prepared to go forward to the witnesses at the appropriate time.

Chairman SHELBY. Senator Allard.

STATEMENT OF SENATOR WAYNE ALLARD

Senator ALLARD. Thank you, Mr. Chairman, for holding this important hearing regarding identity theft. I have been following this issue closely over a number of years, and look forward to hearing from our witnesses.

For many of my constituents, identity theft is something that they believe will never happen to them. However, according to the Federal Trade Commission, in 2004, 246,570 people suffered from a stolen identity, and 4,409 of those cases were my constituents in Colorado, making the State the fifth highest in the Nation.

Identity theft is becoming common to the point that I suspect that many of us in this room know a friend or family member who has had their identity stolen. This presents a grave situation for unsuspecting Americans and a challenge for all financial institutions in the United States.

While there is a need to protect sensitive personal information from getting into the wrong hands, there is also a need for a certain degree of transparency in order for the U.S. financial system to function. The passage of recent legislation, including the FACT Act in 2003, has mandated that consumers be notified of information sharing between various credit reporting agencies. A recent GAO report stated that the implementation of such laws is going well, but it is too early to determine how successful these new laws will be in preventing more cases of identity theft.

I look forward to hearing updates from the industry on these issues, and Mr. Chairman, thank you for holding this hearing.

Chairman SHELBY. Senator Reed.

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman, for holding this hearing, along with Senator Sarbanes, and this is indeed a very important topic. Identity theft is America's fastest-growing

crime. Last year, 9.9 million Americans were victims of identity theft at a cost estimated to be about $5 billion. We live in a time when proliferation of information through various electronic modes of exchange offers extraordinary opportunities to reshape our culture and our economy, but the down side, of course, is we open ourselves up to the exploitation of that information by criminals and by others.

This is especially the case when safeguards are not in place to protect the security and integrity of the electronic information.

We are here to discuss the state of large-scale security breaches leading to compromised personal data and the role that the financial industry can play in preventing these types of breaches, and each of these breaches have affected millions of individuals throughout the country.

We have learned of many data breaches in the past year, where companies have announced that there were significant breaches. Hackers broke into databases belonging to these communities and stole names, passwords, addresses, Social Security numbers, and driver's license information. But in many of these cases, it is troubling to read in the media that companies have learned of intrusion weeks before disclosing the incident, and that if it were not for specific State laws such as the California law, that companies' breaches may never have been reported and would have gone unnoticed and unreported.

Even with the zero liability policies of many major credit card, debt cardholders could see their bank accounts depleted in the interim. So we do have to do much.

I commend the banking agencies for taking a step forward in the right direction by revising their guidance originally issued under Section 501(b) of the GLB Act, Gramm-Leach-Bliley Act, concerning the security of customer information, and the revised guidance requires banking institutions to notify their customers of breaches of security of sensitive information relating to those customers, and that timely disclosure of such breaches will allow the Federal Government, along with the institutions and consumers to closely monitor transaction information and mitigate any resulting damage from the breach.

We have a unique challenge to face in this regard. I hope we can adapt our law to emerging technology which seems to be changing with each passing day, and again, I hope the Government and private industry can increasingly collaborate to stem the threat of identity theft, and look forward to today's hearing.

Thank you, Mr. Chairman.

Chairman SHELBY. Senator Dole.

STATEMENT OF SENATOR ELIZABETH DOLE

Senator DOLE. Thank you, Mr. Chairman. This is indeed a critical issue, and I certainly hope the American public is paying close, close attention to the fact that identity theft is very real and very prevalent.

Identity thieves are constantly looking for new scams to rip off hard-working, law-abiding Americans. And, the stakes could not be higher for the security of the families we represent.

In fact, I will be hosting a workshop in Raleigh, North Carolina the next month or so to educate North Carolinians on the ways to prevent identity theft and what to do if, heaven forbid, they become a victim.

As already mentioned, identity theft is often cited as the fastest growing crime in the Nation. A large portion of the victims include our senior citizens. According to a recent FTC survey, approximately 10 million Americans as we have heard of, victimized by identity thieves every year, at an astonishing cost of $48 billion to businesses, and an additional $5 billion to consumers.

The survey focused on two major categories of identity theft, first the misuse of personal accounts, and second, the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, including the time and money spent resolving the problems. For example, although people who had new accounts opened in their names made up only one-third of the victims, they suffered two-thirds of the direct financial harm. The FTC survey also found that victims of these two categories, cumulatively spent almost 300 million hours, or an average of 30 hours per person, correcting their records and reclaiming their reputation for good credit.

Precise statistics are unfortunately not available to properly gauge the full extent of the problem, since some 40 percent of identity theft cases are believed to involve friends or family members and are never reported.

While financial institutions are liable for the larger part of identity theft fraud, consumers are hurt in more profound ways. In addition to the hours and hours spent reversing the damage, they bear the burden of the insecurity, the inconvenience, and the resulting loss.

A gentleman from Cary, North Carolina told the *Raleigh News and Observer,* "I wouldn't wish it upon my worst enemy." He went on to describe the mess of trying to restore his credit, being turned down for a credit card, having to pay a higher interest rate for a car loan because of his damaged credit. "The hardest thing," he said, "was feeling powerless to do anything once the fraud started to happen." There can be no doubt that when fraud is committed, every law-abiding citizen loses.

Consumers are left to foot part of the bill through the higher cost of services from financial institutions. In March, this Committee held a hearing that focused on two cases in which institutions made public disclosures, as we have heard, with regard to data security breaches. At that hearing, we heard testimony from the Chair of the Federal Trade Commission, who detailed a very reasonable position on this subject, and testified that Congress should consider requiring prompt notification only when there is a significant risk to consumers. This makes sense. Unnecessary notifications could scare consumers, as well as numb them to the risks, and such notification carries a great cost.

As a former FTC Commissioner, I have a great deal of respect for their views.

I look forward, Mr. Chairman, to working with my colleagues to ultimately pass legislation that requires such disclosures when there is a significant risk to consumers.

Thank you.

Chairman SHELBY. Senator Bunning.

STATEMENT OF SENATOR JIM BUNNING

Senator BUNNING. I would like to thank you, Mr. Chairman, for holding this very important hearing, and I would like to thank all of our witnesses for coming before us today. I would especially like to thank and welcome to the Committee our good friend and colleague, Senator Mark Pryor. Thank you for showing up, and we are glad to have you.

Senator PRYOR. Thank you.

Senator BUNNING. This Committee has been a leader on this issue, with Gramm-Leach-Bliley, the FACT Act, and the extensive hearings we have held thanks to you, Mr. Chairman. I appreciate your leadership on this issue, and I am glad we are continuing our good work to assure Americans' financial privacy. These issues should be handled by this Committee. We have the expertise and experience to best deal with privacy issues that affect individuals' financial information and financial institutions. I applaud the Chairman and the Ranking Member for their continued work.

The stories of data breaches that have come to light in the past few years have given all Americans pause. Many of my constituents have taken more and more steps to ensure their financial privacy. They are checking their free credit reports that were provided for in the FACT Act. They are buying paper shredders, and they have made sure the websites they use are secure. Identity theft is a very pressing problem. If the Chairman of the Federal Trade Commission, Deborah Majoras, can become a victim of identity theft, anyone can.

I also understand the fears of the financial services industry. It is very difficult to try and do business and serve their customers, if they have to comply with 50 different State and hundreds of different local financial privacy laws. They can become a liability for noncompliance and for many localities where they have their customers. Also, individuals may not understand their rights. I am not sure how many individuals understand the rights under Gramm-Leach-Bliley and the FACT Act, let alone what rights or prohibitions they may have under State or local laws that may have been passed. Business and individuals need certainty.

However, we must remember that there is a reason why these State and local laws have been passed. Although I am sure many question the motives of politicians, we pass laws because our constituents want them. Given the data breaches that have occurred, and the identity thefts that have happened each year, business must do a better job of protecting private information. We are not at this point today and mistakes have not been made.

Once again, thank you, Mr. Chairman, for holding these hearings, and your dogged efforts on this issue, and thank all of you for coming before us today.

Chairman SHELBY. Thank you.

We welcome our colleague and friend, Senator Mark Pryor from Arkansas, former Attorney General of Arkansas. I think he knew a little about this before he came to the Senate.

Senator Pryor, your written testimony will be made part of the record in its entirety. You proceed as you wish.

STATEMENT OF MARK L. PRYOR
A U.S. SENATOR FROM THE STATE OF ARKANSAS

Senator PRYOR. Thank you very much, Mr. Chairman, and thank you for your leadership on this and the leadership of the Committee. Thank you for the hospitality and for inviting me here to talk today about identity theft and a security freeze.

As Senator Dole mentioned a few moments ago, identity theft is the fastest growing financial crime in the country. According to the Federal Trade Commission, almost 10 million people per year become the victims of identity theft.

In Arkansas, which is a relatively small State, as we all know, identity theft is the top category of reported fraud, with over 1,397 cases reported last year. That does not mean that is all the cases, but is what was reported last year, and in this issue that I first became involved with when I was the State's Attorney General.

According to the Identify Theft Resource Center, it takes about an average of about $1,500 for a person to undo the identity theft, and in some cases we have heard that they have had to spend 600 hours. That is an amazing amount of time, but that is what they have had to expend to try to get out of the mess that someone has created for them.

This crime, it is estimated—I think Senator Dole mentioned this as well—to cost the American business community about $48 billion a year. Just as an example of how our personal information is spread very widely around the country and all of our personal information is, I have right here a stack of about 11 pieces of mail that one of my staff members has received in the last week, 11 pieces in the last week. Only about half of this mail is for him. The other half is for previous occupants of his apartment, and the thing about that is, he knows that when he leaves, a lot of his mail will end up in someone else's hands and he does not know who is going to open that mail, who is going to go through these. A lot of these are for prescreened credit.

So the problem is out there, and there are a lot of different dimensions to it, and certainly I think it is something that the Senate should be very vigilant about. Companies, we all know, we have all read the stories and seen them on television, companies, in the last year or so have had many instances where they have lost data. Sometimes they lose it off a truck, sometimes they accidently expose it, and it is easy to get, sometimes it is stolen from them, but for a while there, as you all remember, there was so much of that going on, that it seemed like almost every other day someone was coming out with a new story.

I think it is just very important that consumers have a tool where they can protect themselves. What I would hope this Committee would consider is the security freeze, and that is one reason that I have pushed S. 1336, the Consumer Identify Protection and Security Act of 2005, because what it allows consumers to do, Americans to do, it allows them some tool that they have at their disposal, totally voluntary, where they can put a security freeze on their information. The way it would be set up would be fairly sim-

ple, where they could put this security freeze out there and then no one could have access to their credit information without them saying so.

Now, honestly, we need to understand this. Some of these companies like to provide instant credit, like right here, you are prescreened, you are preapproved, and all of that. That may not work for people who do not want to receive these. That means that these companies may not be able to do the prescreening but it is almost like signing up for a do-not-call list. If you are going to go to the trouble of signing up for do-not-call, chances are you are not going to be a very good potential customer for a telemarketer. This is the same thing as here. Chances are these people are not going to be very good potential customers here.

Right now, what we are starting to see is States taking action. You have California, Louisiana, Texas, Vermont, and Washington that have the law. Maine and Nevada, looks like they are going to come on in the next couple of months. There are a number of other States. I think it is 20 some odd States that are considering the law this year, and so what is happening out there is you are getting this thing that we see a lot, this patchwork quilt around the country. Even though I like States to have the authority to do things, under this circumstance it might be better—I believe it is better—to have a Federal system that everybody can tap into. If nothing else, the credit bureaus then have one system that they have to comply with, not 50 different systems.

Also technology and the technology sector is going to respond to this. There is a company out in California that is trying to set up some software for one-stop-shopping that will be very easy for consumers to use, so it looks like the marketplace is going to adjust to this. I think it is going to be a win-win for everybody.

This Committee will consider a lot of different factors when they look at this. I appreciate your time and your deliberation on this, but I do think it is important for the Senate to act, and that we try to show some leadership on this because it is just too big of a problem that is growing every single year, as Senator Dole said a few moments ago.

We do have the ability to do this, and our inaction would just make a bad situation worse out there.

Mr. Chairman, thank you for that, and thank you for allowing my full statement to be part of the record.

Chairman SHELBY. Thank you. I understand you have Committees you have to attend. We appreciate your appearance.

Senator PRYOR. Thank you very much.

Chairman SHELBY. Our second panel will be Mr. Stuart Pratt, President and Chief Executive Officer, Consumer Data Industry Association; Mr. Ed Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group; Mr. Ira Hammerman, Senior Vice President and General Counsel, Securities Industry Association; Mr. Gilbert Schwartz, Partner, Schwartz & Ballen, LLP; and Mr. Oliver Ireland, Partner, Morrison & Foerster.

Gentleman, you take your seats. All of your written testimony will be made part of the hearing record in its entirety. We will start with you, Mr. Pratt, for you to briefly sum up your top points.

STATEMENT OF STUART K. PRATT
PRESIDENT AND CHIEF EXECUTIVE OFFICER,
CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Chairman Shelby, Senator Sarbanes, Members of the Committee, thank you for this opportunity to appear before you today. For the record, I am Stuart Pratt, President and CEO of the Consumer Data Industry Association.

Mr. Chairman, we commend you as well for holding this hearing. It is an important subject and one on which we welcome the chance to share our views.

I am very pleased to announce on behalf of CDIA's members, Equifax, Experian, and TransUnion, a new initiative focusing on encryption of data reported to them. As of today, any furnisher of information can choose one of a number of acceptable encryption standards for use with all three companies by offering a data furnisher the choice to use one encryption standard. We reduce costs. We simplify the administration of encryption. It is our hope that with these new encryption standards in place, we will accelerate the choice to encrypt data that is supplied to consumer reporting agencies, and ultimately to achieve the goal of all information being encrypted when it is transmitted to us.

Now let us take a look at the FACT Act that has been mentioned a number of times, and we believe it materially does add to the protections of consumers through the Uniform National Standards that were established through the leadership of this Committee in particular. Fraud alerts, for example, we believe often strike the right balance for consumers who wish to ensure that a lender is notified of their concerns about identity verification. I think consumers recognize fraud alerts slow down the process. They do not stop the transaction, however. In fact, the FACT Act strengthened the fraud alert system on members that had voluntarily established by making a responsibility of the receiving party that they must take additional steps to verify the identity of a consumer when a fraud alert is present. The FACT Act also addressed the needs of active military service personnel through a special alert that can be added to the credit report as well.

Address discrepancy indicators was another idea that was enacted through the FACT Act. This duty requires us, the nationwide consumer reporting agencies, to indicate to a lender, when they request a credit report, when the address they have submitted to us differs substantially from the address we have in the file. It is a very practical idea. It is a good idea. We were glad to have been able to put that into place by December 1, the effective date, in 2004.

Identity theft reports was a particularly important addition because consumers at times had trouble obtaining police reports in order to take advantage of rights they had under the law. The report is more flexible and allows consumers to obtain a report from any one of a number of law enforcement agencies.

Ultimately, I think Congress was prescient in recognizing that fraud prevention identity theft victim assistance are best handled through uniform national standards, and it remains critical to our members who are operating as consumer reporting agencies, that

we remain regulated solely under a single set of law and regulation, and that would be the Fair Credit Reporting Act.

You have asked for our views on sensitive personal information that is held by nonfinancial institutions, and we have really two key themes in that regard, ensuring the security of information and sending consumers meaningful notices when there is a breach of that information.

It is our view that a rational and effective national standard should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a financial institution or not.

Information security standards that are substantially similar to those we see in the GLB are well-suited for this type of regulation, and we would encourage this Committee to continue to look into that. To ensure regulatory continuity, we believe if there are new provisions established, these provisions would therefore also deem a financial institutions as being in compliance with those standards because of their compliance already with the GLB standards.

For consumers and notification, we believe consumers should receive notices when their sensitive information is breached, and when there is a significant risk of harm, and in fact, key to notification requirements is making sure they do not result in either over-notification, but equally important, too few notices being sent.

Chairman SHELBY. When you say receive it, receive it immediately?

Mr. PRATT. In terms of the notice, sir?

Chairman SHELBY. Yes.

Mr. PRATT. I am sorry, I should have brought another set of glasses so I can see at the same time I am reading my testimony, but I think we would say that in concert with law enforcement investigations, Mr. Chairman, just to make sure that we do not open the door too soon before they have shut down the problem. I think that is the only coordination issue that we would raise with you, Mr. Chairman.

Chairman SHELBY. Thank you.

Mr. PRATT. I think key to notification is the trigger, when do you send that notice? Chairman Majoras suggested, and got it right, when she said that a trigger should pivot off of a significant risk of harm. We think significant risk of harm is best defined as a risk of being a victim of identity theft, the very subject of this hearing.

We also need coordination with national credit bureaus if thousands of notices are being sent out the door by many different agencies, many different companies, many of whom we do not have business relationships with. It is our job to plan and be able to handle the contacts that come back to us. We need some coordination. We would ask for that to be included in a proposal of this sort.

You have asked us to also discuss file freezing, and we provide the following background. File freezing, as Senator Pryor has discussed, allows a consumer to freeze his or her credit report for I think what we would call new business purposes. File freezes have been enacted in 12 States. The file freeze enactments do often allow a consumer to charge a fee. Certainly, we have been on record in many States as indicating concerns about the rigidity of file freezes, how operable they will be for consumers, but I will tell

you at this point, with this many enactments in the States and with many State legislatures looking at this next year, we encourage this Committee to continue to look at what we now have, and preserving what we now have, which is a seamless nationwide credit reporting system servicing a nationwide credit system in this country.

And that is a dialogue that needs to continue in the context of these State laws, and it is a dialogue that needs to continue. It is an extension of the good work of this Committee in creating national standards through the FACT Act.

With that, Mr. Chairman, I will close my opening remarks. Thank you, sir.

Chairman SHELBY. Thank you.

Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI
CONSUMER PROGRAM DIRECTOR,
U.S. PUBLIC INTEREST RESEARCH GROUP
ON BEHALF OF
CONSUMER FEDERATION OF AMERICA, CONSUMERS UNION,
ELECTRONIC PRIVACY INFORMATION CENTER,
PRIVACY CONSULTANT MARI FRANK,
PRIVACY RIGHTS CLEARINGHOUSE, PRIVACY TIMES,
U.S. PUBLIC INTEREST RESEARCH GROUP, AND
WORLD PRIVACY FORUM

Mr. MIERZWINSKI. Thank you, Chairman Shelby. I am Ed Mierzwinski, the Consumer Program Director of the U.S. Public Interest Research Group. My testimony is also on behalf of a number of consumer and privacy groups, including the Consumer Federation, the Consumers Union, the Privacy Rights Clearinghouse, and EPIC.

I want to commend you for your longstanding leadership on privacy, along with Senator Sarbanes for his leadership, particularly on the Sarbanes Amendment, which allowed States to go further with financial privacy laws to the Gramm-Leach-Bliley Act.

We would not know about the nearly 100, depending on whose list you look at, security breaches that have occurred this year if it were not for the pioneering efforts of California in enacting a security breach notification law. Because the States have demonstrated such leadership on security breach notification laws, we believe the Committee should look very carefully, if it is going to enact any breach notification provisions, at maintaining only a Federal floor and allowing the States to continue to go further.

As another example of how the States have shown leadership and how our nonuniform system has worked well, I would point out that the FACT Act allows States to go further in identity theft areas. Although our groups were disappointed that you did not allow States to go further in all areas, the FACT Act did allow States to pass stronger identity theft laws, and that is why a number of States, a dozen so far—and New Jersey is signing its law today—have enacted security freeze legislation around the country.

Chairman SHELBY. How would a security freeze work exactly?

Mr. MIERZWINSKI. A security freeze really is the first way that we can give consumers control over their confidential person infor-

mation, Senator Shelby. Most of the protections that are given to consumers in the FACT Act are protections after you have already become a victim—the right to a fraud alert, the right to clear your name, that type of thing. Identity thieves take advantage of the easy availability of Social Security numbers, coupled with the way that creditors apply for credit reports, and obtain them in your name to obtain credit in your name at a creditor's. A security freeze gives you the right to freeze access to your report for any new creditors. It essentially leaves the thieves out in the cold, but your existing creditors can still look.

Chairman SHELBY. But in the FCRA, we use fraud alerts instead of that, I believe.

Mr. MIERZWINSKI. We use fraud alerts, but, again, a fraud alert is after you have already become a victim or suspect you are a victim. A freeze, in our view, should be available to everyone in advance. It essentially puts your credit report in a freezer so that the bad guy applies for credit in your name, and the creditor says, "We cannot get a credit report on you." So you are protected. You can sleep at night.

Chairman SHELBY. So it is working.

Mr. MIERZWINSKI. We think it is working. We would prefer that the freeze be easier to do, that it be cheaper, that it be selectively unfrozen, that you could turn it on and leave it on, but then, for example, on a Saturday if you are looking for cars, you should be able to selectively unfreeze it for car dealers just for the day. We have instant credit. Why can't we have an instant freeze? That is really what we are looking for.

Getting back to the issue of the security breach, which is on Congress' mind because of all the security breaches that have occurred, I first want to point out that a lot of the companies have claimed that they were victims. Well, I am shocked to hear that. CitiFinancial, an arm of CitiGroup, and Bank of America both lost unencrypted data tapes containing records of millions of Americans. Other banks have lost laptops that were unencrypted containing records on many Americans. ChoicePoint sold its records. It did not lose them. It sold records to a thief. So we have some real problems out there with the way industries are taking care of our information. And the notion of a harm trigger is, I think, one that has been debated almost as much if not more than preemption of State law.

Our view, the consumer coalition that I represent, is that if you lose the information, there should be disclosure to the consumer. That will, number one, force the companies to do a better job in the first place; but, number two, it will give consumers knowledge that their personal information has been lost. The problem has been that half of consumers do not know how they became identity theft victims.

Chairman SHELBY. But all this requires changes in statutes, statutory change?

Mr. MIERZWINSKI. Well, I think that if you were to enact a security breach law, your Committee, the bank regulators have already enacted a breach regulation that applies to financial institutions under their regulation.

Chairman SHELBY. They did that by regulation.

Mr. MIERZWINSKI. By regulation, by guidelines actually. But for other types of entities, ChoicePoint is not regulated by the bank regulators, nor are these card processors. So they would require additional legislation.

My written testimony, Mr. Chairman goes into a number of other details on improvements to the FACT Act. For example, we believe that breach victims should have the right to obtain fraud alerts more easily, that extended fraud alerts should be more easily available, that police reports should not be required for a consumer to obtain business information. We also list a number of recommendations that may not be in the purview of the Committee, but I know are of very much interest to you, to improve Social Security number protection and get our financial DNA out of the marketplace so that the thieves cannot get at it.

I appreciate the opportunity to testify before you today, and I want to point out that my written testimony includes a list of the major breaches that have occurred this year as Appendix 1. It includes a list of all the State security breach laws and a list of all the State security freeze laws.

Thank you.

Chairman SHELBY. Thank you.

Mr. Hammerman.

STATEMENT OF IRA D. HAMMERMAN
SENIOR VICE PRESIDENT AND GENERAL COUNSEL,
SECURITIES INDUSTRY ASSOCIATION

Mr. HAMMERMAN. Mr. Chairman, Ranking Member Sarbanes, and Members of the Committee, I am Ira Hammerman, Senior Vice President and General Counsel of the Securities Industry Association, and I appreciate the opportunity to testify on our industry's responsibility to prevent identity theft and protect our customers' financial information. We applaud your leadership and foresight, Mr. Chairman, and that of Senator Sarbanes in passing the precedent-setting law for data security, the Gramm-Leach-Bliley Act of 1999. Maintaining the trust and confidence of our customers is the bedrock of the securities industry. The long-term success of our markets depends on customers feeling confident that their personal information is secure. We, therefore, devote enormous time and resources to the protection of customer data. We are, however, concerned that the expanding patchwork of State and local laws affecting data security and notice will make effective compliance very difficult for us and equally confusing for consumers.

The problem of data security is a distinct Federal responsibility that requires a targeted Federal legislative and regulatory response. In light of the increasing number of disparate Federal and State legislative proposals, we urge this Committee to strike the appropriate balance between addressing the legitimate concerns of American consumers threatened by identity theft and ensuring that protections are indeed meaningful.

All businesses that have custody of sensitive personal information have a responsibility to provide data security measures. It is our belief businesses have a similar obligation to notify consumers when a breach of security creates a significant risk to their identity.

As the Committee is well aware, the securities industry is subject to Securities and Exchange Commission regulations that requires every registered broker-dealer to have in place policies and procedures to safeguard sensitive customer records and information. The SEC and the self-regulatory organizations periodically examine broker-dealers to ensure compliance with this regulation. Similarly, the SEC has full authority to issue relevant guidance on how to construct a notification regime that best benefits consumers, and SIA looks forward to working with SEC Chairman Cox and his staff in determining how best to develop such a regime.

In considering legislation related to data breach, SIA urges the Committee to consider the following six principles: First, adopt a clean National standard to achieve a uniform, consistent approach that meets consumer expectations; second, implement a trigger for consumer notice that is tied to significant risk of harm or injury that might result in identity theft; third, a need for a precise definition of sensitive personal information that is tied to the risk of identity theft; fourth, exclusive functional regulator oversight and rulemaking authority; fifth, a flexible notification standard; and, finally, reasonable administrative compliance obligations.

SIA urges the Committee to develop meaningful and carefully targeted legislation that embodies these important principles.

The securities industry recognizes that we face a major threat from criminals, including potential terrorists, who perpetrate identity theft. Therefore, we take very seriously our duty to safeguard our customers' sensitive financial information. Identity theft and other kinds of fraud hurt not only consumers but also businesses whose reputations inevitably suffer from security breaches. The cost of fraud is often beyond the monetary. Lost customers and reduced confidence can be the death knell for a business so dependent on the public's trust.

Thank you again for the opportunity to testify today. We are eager to work with the Committee and its staff to draft meaningful and targeted effective data breach legislation. Thank you.

Chairman SHELBY. Mr. Schwartz.

STATEMENT OF GILBERT T. SCHWARTZ
PARTNER, SCHWARTZ & BALLEN LLP,
ON BEHALF OF
THE AMERICAN COUNCIL OF LIFE INSURERS

Mr. SCHWARTZ. Chairman Shelby, Ranking Member Sarbanes, and Members of the Committee, I am Gilbert Schwartz, Partner in the Washington law firm of Schwartz & Ballen, and I am appearing today on behalf of the American Council of Life Insurers, the principal trade association for the Nation's life insurance industry. ACLI's 356 member companies account for 80 percent of the life insurance industry's total assets in the United States.

This hearing today represents another chapter in the Committee's longstanding leadership in this area and strong commitment to the protection of consumer information and to the prevention of identity theft, as evidenced by the Committee's central role in the enactment of the Gramm-Leach-Bliley Act and the FACT Act. ACLI appreciates the opportunity to discuss the important role

that life insurers play in preventing identity theft and protecting financial information of our policyholders.

Life insurers have long been committed to establishing and maintaining policies and procedures to protect sensitive customer information and to prevent misuse of such information. Insurers expend considerable resources to achieve these goals. ACLI and its members were, and continue to be, strong supporters of Title V's privacy and information security provisions.

As a result of the Gramm-Leach-Bliley Act, 34 States have adopted comprehensive regulations or statutes that establish standards for safeguarding customer information by insurers. The State requirements generally track the National Association of Insurance Commissioners' Standards for Safeguarding Customer Information Model Regulation. Under the NAIC model reg, life insurers are required to adopt comprehensive security programs to protect customer information.

In 2003, Congress enacted the FACT Act in part to respond to the growing crime of identity theft. Because of recent concerns with the possibility of identity theft resulting from security breaches, 20 States have enacted legislation requiring companies to notify consumers in the event that sensitive personal information is affected by a security breach. Some States' notices require differences in scope and coverage. As Senator Pryor indicated, this is a patchwork quilt. The need to track these differences and factor them into a notification program will inevitably make it more difficult for institutions to send notices to consumers promptly. This may cause some consumers to experience delays in receiving notices and increase the likelihood that they will become victims of identity theft.

Varying State laws may also result in uneven enforcement from State to State. Accordingly, ACLI supports Federal legislation that provides preemptive uniform national standards for notifications to individuals whose personal information has been the subject of a security breach where such information may lead to substantial likelihood of identity theft. Such an approach benefits consumers because it ensures that they receive the same information in a timely fashion, regardless of where they reside.

ACLI also recommends focusing on breaches involving sensitive consumer information that is not encrypted or secured by a method that renders the information either unreadable or unusable. To avoid needlessly alarming consumers and undermining the significance of these notices, ACLI supports notification when there is a significant likelihood of identity theft. Uniform enforcement of notification standards is very important. ACLI strongly supports enforcement of insurers' compliance exclusively by the Department of the Treasury. Treasury is well-positioned to assume this role because it has had extensive experience with the insurance industry in connection with such laws as the USA PATRIOT Act, the Terrorism Risk Insurance Act, the Bank Secrecy Act, and OFAC regulations.

In the event it is not possible to provide for enforcement by the Treasury Department, ACLI supports adoption of an approach set forth in the GLB Act. Under this approach, an insurer's compliance with Federal breach of security notification legislation would be enforced by the insurance authority of the insurer's State of domicile.

If this approach is used, ACLI also requests that the legislation state that it is the intent of Congress that State insurance authorities enforce the legislation in a uniform manner.

If the legislation provides for implementing regulations, ACLI believes that the relevant Federal agencies should jointly promulgate the rules. This would benefit consumers and assure that they will receive the same protection across all industries.

The issues before you today, Mr. Chairman, are complex. ACLI anticipates that legislation you adopt will provide meaningful protection to consumers who might otherwise become victims of identity theft.

Thank you for your attention.

Chairman SHELBY. Thank you, Mr. Schwartz.

Mr. Ireland.

STATEMENT OF OLIVER I. IRELAND
PARTNER, MORRISON & FOERSTER,
ON BEHALF OF THE
AMERICAN BANKERS ASSOCIATION

Mr. IRELAND. Chairman Shelby, Ranking Member Sarbanes, and Members of the Committee, my name is Oliver Ireland, and I am a Partner in the DC office of Morrison & Foerster. I am here today on behalf of the American Bankers Association to address the role of banks in protecting consumers from identity theft and account fraud.

The American Bankers Association includes community, regional, and money center banks and holding companies, as well as savings associations, trust companies, and savings banks, and it is the largest banking trade association in the country.

We appreciate your leadership in the area of privacy and identity theft and the opportunity to participate in this hearing. Identity theft occurs when a criminal uses information relating to another person to open a new account in that person's name. In addition, information relating to consumer accounts can be used to initiate unauthorized charges to those accounts. The issue of identity theft and account fraud are of paramount importance to banking institutions and the customers that they serve.

In this regard, I would like to emphasize three key points: Banks have a vested interest in protecting customer information and are highly regulated in this area; a uniform approach to information security is critical; and any security breach notification requirement should be risk-based.

First, banks have an interest in protecting customer information. Simply put, banks that fail to maintain the trust of their customers will lose those customers. In addition, because banks do not impose the losses for fraudulent accounts or fraudulent transactions directly on their customers, banks incur significant costs for identity theft and account fraud. These costs are in the form of direct dollar losses as well as reputational harm. Accordingly, banks aggressively protect sensitive information relating to consumers. Among those that handle and process consumer information, banks are among the most highly regulated and closely supervised.

Guidance under Title V of the Gramm-Leach-Bliley Act requires banks not only to limit the disclosure of consumer information but

also to protect that information from unauthorized access and to notify customers when there is a breach of security of sensitive customer information. In order to provide consistent protection for consumers, merchants, information brokers, and others that handle sensitive customer information should be subject to similar requirements.

In designing security notification requirements, national uniformity is critical to preserving efficient national markets. A score of State legislatures have already passed new data security bills. While these laws have many similarities, they also have important differences. State laws that are inconsistent result in both higher costs and uneven consumer protection. Further, a single State that adopts a unique requirement or omits a key provision can effectively nullify the policy of other States.

Finally, any notification requirement 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. Any security breach notification requirement should be limited to those cases where the consumer needs to act to avoid substantial harm. Further, security breach notification requirements should be tailored to the particular circumstances and the threat presented.

Identity theft and account fraud pose different risks. In each case, the need for notification and the form of the notification will differ. Any Federal legislative requirement must recognize and accommodate these differences.

Banks are proud of their record in protecting information relating to their customers and will continue to work to ensure that consumers receive the highest level of protection.

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

Chairman SHELBY. Thank you, Mr. Ireland.

I will direct my first to Mr. Pratt. Do you believe that the fraud alert scheme that we included in the FCRA can work in tandem with the various State credit freeze laws that have been enacted in recent years that we have discussed here?

Mr. PRATT. There is no doubt that credit freeze laws do not prohibit, if you will, a credit reporting agency from also putting a fraud alert on the file, so that fraud alert could be conveyed to a bank, for example, that has a current business relationship and is accessing the credit report for that purpose. But the fraud alert system is a more flexible system. It is a system that allows the transaction to go forward under a caution flag. A file freeze, as has been described—and I think rightly so—is an absolute stop. It will stop the transaction cold in its track. File freezes, by the way, are not absolute. You can lift a freeze for a temporary period of time, and this is a consistent element of the laws that we have seen in the States. But you have to do that in advance of the transaction in which you intend to engage.

Chairman SHELBY. Ed, do you have any comments on that? Can they work together?

Mr. MIERZWINSKI. I agree with everything that Stuart said there. The two are separate rights; the two are separate protections. Again, the freeze, as Stuart pointed out, anyone, regardless of

whether you have been a victim or think you are threatened by identity theft, can impose a freeze. A fraud alert you put on after you think you have been a victim, and the company must take additional steps before issuing credit.

Chairman SHELBY. Is a freeze, in a sense, preemptive?

Mr. MIERZWINSKI. Preemptive, in the other sense of preemptive, yes.

Chairman SHELBY. Okay.

Mr. MIERZWINSKI. It is often used around Capitol Hill, too.

Chairman SHELBY. Mr. Ireland, do you have any concerns about the impact that the use of credit freezes could have on the credit reporting system, the users of credit reports, or consumers? In other words, will there be an impact here if a freeze continues?

Mr. IRELAND. There is a significant potential for impact in this area. We saw some examples earlier of prescreened solicitations and the possibility that prescreening as a process could be disrupted. I think perhaps more significantly there are other credit transactions that occur with little prior notice, including opening credit charge accounts at retail outlets, automobile purchases, and so on, that are likely to be disrupted by a security freeze process. And the consumers, when they place those freezes, may well not understand that that is going to occur and may not remember to remove them in time.

Chairman SHELBY. Mr. Ireland, I think it is important to go over just some of the basic, elemental questions associated with the situation where information held by financial institutions is compromised.

First, what, if any, different distinction should we make based on the kind of information that has been compromised? In other words, does the type of information that has been disclosed matter?

Mr. IRELAND. I think the type of information is critical.

Chairman SHELBY. Give us an example.

Mr. IRELAND. There is an initial issue as to whether you want to merely protect the privacy of consumer information with notifications or you want to be concerned about alerting consumers when they need to protect themselves, take action to protect themselves from identity theft or fraud. Much information about consumers cannot be used for either identity theft or account fraud, and while it is desirable to protect that information from unauthorized use, providing notices to consumers about disclosures of that information that may be unauthorized runs the risk of inundating them with notices, so that when a final notice does come that they need to do something, they miss it.

Chairman SHELBY. Should the nature—in other words, the security breach you alluded to—matter?

Mr. IRELAND. I think the nature of the security breach also matters. It matters in terms of the information. The nature of the security breach also matters in terms of determining whether harm will result. There are security breaches that occur which are for competitive purposes in financial markets where there is no risk of identity theft or fraud associated with it.

Chairman SHELBY. If you have different situations here, how should the differences be dealt with in relation to the type of notice provided to consumers?

Mr. IRELAND. The classic example is the difference between account fraud and identity theft information. If somebody loses name, address, and Social Security number, the thief can go open an account at another institution, and the consumers need to check their credit report to determine whether that happens. As Mr. Pratt has already indicated, in those cases coordination with the credit reporting agencies is appropriate and may be necessary. And the consumer has to take action with the credit reporting agencies.

If the information is merely account number and name, it might be used to commit account fraud, but the credit reporting agencies need not be involved in that matter.

Chairman SHELBY. Mr. Hammerman and Mr. Schwartz, I will direct this question to you two. The financial institutions that you represent have duties under the Gramm-Leach-Bliley Act to protect sensitive consumer information. However, I would assume protecting consumers and yourselves is not merely a question of complying with the law and that you have to be more proactive in response to the threats that exist. You know there are threats out there. Is it true that you could highlight some of the efforts that you undertake as being proactive in your area?

Mr. SCHWARTZ. Certainly. Insurers have robust systems and procedures in place: Who can have access to the information in terms of encryption keys that are placed on information, who has access to buildings where some of the data are collected, how that information may be processed in various circumstances. And there are a whole range of actions that are put into place that ensure that only information will be made available when the appropriate parties are asking for it.

So we are very confident that the insurance industry has state-of-the-art protections in place and is constantly trying to upgrade and ensure that whatever is developed is put into place as well. Encryption devices are always being upgraded as hackers try to break those encryption keys, and new procedures are implemented all the time.

Chairman SHELBY. Mr. Hammerman, do you have any comments?

Mr. HAMMERMAN. Yes, Mr. Chairman. I think this issue first starts with getting senior management support for data protection, and we have that among our members.

In addition, there are dedicated groups of people within each firm whose sole job is to handle information security and privacy. As was mentioned, our firms have strong perimeter defenses to protect their networks. We are constantly utilizing technology to try and anticipate the next problem, and we are always trying to stay one step ahead——

Chairman SHELBY. But the thieves also use technology, do they not?

Mr. HAMMERMAN. I was just going to say that we try to stay one step ahead of them, and it is constantly changing. But we are putting the resources set forth to do that.

Chairman SHELBY. Senator Sarbanes.

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

I have a couple of very simplistic-sounding questions to put first to the members of the panel.

Senator DODD. Be careful.

[Laughter.]

Senator SARBANES. If I am in a State which has passed additional legislation on this issue, providing additional substantive standards guarding me against identity theft, and a national law is passed which preempts State law, and the substantive standard in the national law is less, lower than the protections provided under my State law, I will have lost consumer protection, will I not?

Mr. MIERZWINSKI. Senator, I would agree that you have lost consumer protection. I would also point out that under the current regime that we have the California law has effectively been adopted nationwide by State Attorneys General. After the ChoicePoint breach, when California citizens started receiving notices, the State Attorneys General of other States told ChoicePoint, "What about our citizens?" And they provided notice nationwide. And so the opposite has occurred. You have more rights in States. So that argues for not preempting.

Senator SARBANES. I want to address this argument which I heard that a preemptive Federal law, would provide more consumer protection. And I have trouble understanding that except in a State that has no consumer protections whatsoever, perhaps. Whether it does or not would depend directly upon the substantive standard in the Federal law, would it not?

Mr. SCHWARTZ. Yes, that is correct, Senator Sarbanes.

Senator SARBANES. So if the Federal standard is weak, or indeed fairly strong but not as strong as the State standards, at least if I am a consumer in a State that has enacted legislation, I will actually lose protection, not gain protection. Is that correct?

Mr. SCHWARTZ. Senator, I think it depends upon the nature of the State provisions. I think many of the State provisions are different from State to State. It is not that necessarily one is regarded as stronger but, rather, it is different. And, for example, if the nature of the information that is the subject of a particular State's legislation differs from another State, as Senator Pryor indicated, you end up with a patchwork quilt. And, in fact, you end up perhaps resulting in a delay in informing the consumer until the company can figure out exactly what information was taken and whether or not that particular State law applies to that information.

I think that it is really a compliance issue that, unfortunately, given the differing State laws, could very well result in less consumer protection, not more for that particular consumer in the State.

Senator SARBANES. Are you telling us that there is a very significant compliance issue, that these data collectors, who presumably have very sophisticated means of data collection, retention, cross-filing, and all the rest of it, cannot comply with varying State laws?

Mr. SCHWARTZ. I am not saying they cannot comply with the varying State laws. It makes it much more complex, and it takes them more time to comply with State laws that differ from place to place. A uniform Federal statute that addresses the identity theft provisions and provides for notification to consumers can be very well-tailored and be done promptly as opposed to having to de-

cide and do an investigation to determine whether that particular breach falls within that particular State's law. And if you have 50 different State provisions, it could result in a significant time lag.

Senator SARBANES. Would you anticipate that the substantive Federal standard, if you moved in that direction and were to preempt, would be at least as strong as the existing California standard or even stronger?

Mr. SCHWARTZ. I think we would have to look at the provisions. I think it has to be tailored to specific problems of identity theft, and California was the first one that passed and it perhaps needs some tweaking.

Senator SARBANES. In which direction?

Mr. SCHWARTZ. In the direction of assuring that it identifies the problem and is directed toward solving the problem as opposed to being over-inclusive.

Senator SARBANES. So you think the California standards at the moment are too strict and rigid. Is that correct?

Mr. SCHWARTZ. I would have to take a look at them and compare them to what is being proposed. But I do think, for example, if you have to provide a notice for a breach of all information, you end up receiving so many notices in the mail that, if I were a consumer, I would completely ignore them because I am receiving one for any type of breach even though it may not result in any harm to me.

Senator SARBANES. Well, that leads me into my next question, if I could.

Chairman SHELBY. Go ahead, Senator Sarbanes.

Senator SARBANES. I won't be long.

Mr. Ireland, I am reading your testimony, and I notice you make reference to the guidance which the Federal banking agencies have issued and the final Interagency Guidance on Response Programs for Unauthorized Access to Customer Information.

Mr. IRELAND. That is correct.

Senator SARBANES. The standard there is to notify its affected customers where misuse of the information has occurred or is reasonably possible. Is that correct?

Mr. IRELAND. That is correct.

Senator SARBANES. But I take it it is your position that it should be that there is a significant risk of harm. Is that correct?

Mr. IRELAND. That is correct.

Senator SARBANES. And that is a higher threshold to cross with respect to notice—would that be correct?—than the existing guidance. If that were the standard, that would diminish the number of notices to provide compared with the current guidance from the Federal banking agencies. Would that be correct?

Mr. IRELAND. I am not sure that would be the case. In the banking agency guidance, there is a process created by which, when a breach occurs, the bank suffering the breach notifies their examiner about the breach, and this is likely to lead and typically does lead to a dialogue about whether or not notice is required. And so you have an ongoing process with the bank regulators about whether or not there is sufficient risk to generate notice. I am not sure that the language in the guidance completely captures that process. I think if you are going to go out and adopt a bill that is supposed to be self-effectuating, that people are going to adhere

without the benefit of that dialogue—and that dialogue really cannot occur in less regulated institutions. You need a crisper line, and I would recommend the significant risk of harm standard there, which I think is broadly consistent with what the banking agencies have done.

Senator SARBANES. Do you think that the guidance they have issued is equivalent to significant risk of harm?

Mr. IRELAND. I believe that generally the way the banking agencies have implemented that has been consistent. I do not have a survey of all of the notifications that have been given under that standard, but I think they are generally consistent.

Senator SARBANES. So you think you already have a risk-based standard. Is that right?

Mr. IRELAND. We think we already have a risk-based standard—

Senator SARBANES. Why in your statement then do you, after you set out the guidance of the banking agencies, say that you believe that a workable notification law would require entities, et cetera, et cetera, to notify individuals upon discovering a significant breach of security? Your statement seems to carry with it the implication that you do not, at the moment, have the significant risk of harm standard?

Mr. IRELAND. We have a standard under 501(b) for customer information that is being implemented as I described through a process. If I were going to try to articulate the results of that process in a bill, as I said, to be self-effectuating, the language I would use to describe it would be "significant risk of harm."

I would also point out that the 501(b) guidance does not capture all of the information that is currently held by banks about consumers, and that if you adopt a bill that requires notification based on security breaches of consumer information, there will be places where that bill would apply to banking information that is not covered by the current guidance.

Senator SARBANES. Mr. Mierzwinski, do you have a take on all of this?

Mr. MIERZWINSKI. Well, the consumer groups and the privacy groups have made it pretty clear that a harm standard or a harm trigger would work against giving consumers greater privacy rights. We think that the California standard is the proper standard to adopt nationally. Lose the information, almost in all circumstances provide the notice. But I would certainly say that the way that you have described the bank regulator guidances is the way we read them and that the industry seeks a higher standard which is much more difficult to attain. And I would respectfully disagree with Mr. Ireland.

One of the other issues with harm triggers is the issue of whether they apply to identity theft, whether they apply to harm, or whether they apply to simple misuse. We believe that information can be misused in many ways in addition to identity theft. Information can be used to publicly embarrass you. It can be used for stalking. It can be used for terrorism. It can be used for criminal identity theft as well as financial identity theft. Account fraud may not be captured by a definition of identity theft.

So there are a lot of problems with any of these triggers. They will all be litigated, and that is just another reason not to use them.

Senator SARBANES. Thank you.

Thank you, Mr. Chairman.

Chairman SHELBY. Senator Dodd.

STATEMENT OF SENATOR CHRISTOPHER J. DODD

Senator DODD. Thanks, Mr. Chairman, and thank you and Senator Sarbanes for holding this hearing and asserting what I think is the appropriate jurisdiction of the Committee over this issue. And I thank Senator Pryor in his absence for submitting some legislation. It is a complicated area, but obviously I was looking over that chart that appeared in the *Washington Post* some time this year—I do not have the exact date on it—which identifies at least in the area of 15 million accounts that have been exposed to the possibility of identify fraud as the result of various problems that have occurred from various institutions, going back to February 15 with ChoicePoint and the identification fees on assessed accounts, 145,000, to, of course, the Card Systems hacker on June 18 of 40 million people. So there is a serious problem, obviously, that hangs out here that needs to be addressed. I think you all recognize and acknowledge that, and that is up to June. I presume those numbers may be even larger today. I do not have that information in front of me. So this is a significant issue and a tremendously important one for people across the country.

I have a couple of issues. I want to get to—the last question I want to ask you about and have you think about this is Katrina and what the credit bureaus are doing for the people in the hard-hit areas of the Gulf States to protect their credit information as a result of what has happened to them, losing a lot of their own documentation, and whether or not there are any problems that are emerging here with identity theft of people in that region because of the devastation that has occurred there.

But I want to pursue two other issues more generally. Under Title V of the Gramm-Leach-Bliley law, financial institutions are required to protect their customers' sensitive personal information where a customer is defined as a person to whom the institution provides a product or service. However, many financial institutions have data and information on people that are not customers. For instance, I apply for a credit card and I provide financial information. I decide or you decide either not to grant me a credit card or I decide to do business with another company. What do you do with that information about me? I am not a customer under Title V of Gramm-Leach-Bliley, but there is a lot of information being held by people out there now that can be misused, that can be the subject of theft. And I would like particularly the representatives of our financial institutions here to comment on what happens to that information that exists.

Mr. IRELAND. Senator, typically banks protect that information the same way they protect customer information.

Senator DODD. Are they required to, in your view, under the law?

Mr. IRELAND. Under the Gramm-Leach-Bliley guidance, I do not think they are required to. Let me make it clear, we are happy to

live with the standards in the Gramm-Leach-Bliley banking agency guidance that we have today, and we are happy to apply that to that additional information maintained by banks as well as the customer information that is currently subject to the guidance.

Senator DODD. But there is no legal requirement of you to do so, the kind of information I just described?

Mr. IRELAND. Not under the guidance. There is no legal requirement under the guidance.

Senator DODD. What is being done on——

Mr. SCHWARTZ. Senator Dodd, with respect to the insurance industry, clearly all that information on applications, whether the insurance policy is issued or not, is protected, just the same way that an insured's information is protected.

Senator DODD. Protected because it is a matter of policy of the insurance industry but not as a matter of law?

Mr. SCHWARTZ. Yes. From a reputational risk standpoint, that information is just as protected and just as valuable from the standpoint of being protected. And, again, the policies and procedures will apply across the board to the information regardless of whether it is a customer or not.

Senator DODD. Do you share that viewpoint?

Mr. HAMMERMAN. Yes, Senator.

Senator DODD. Do you have any comment on this as an area that we should maybe look at here in terms of protection of consumer information?

Mr. MIERZWINSKI. Senator, I think you should look at that area, and our testimony goes into detail about two other areas, one of which you touched on. The third-party processors, such as Card Systems, do not have customers. They are not covered by the GLB Act either, although they may be acting as agents of regulated entities. And I believe that at least one of the card associations has suspended Card Systems for violating its own rules. That may not have been enough. It may have been after the horse had left the barn, but they did do so.

The other big area, of course, are the data brokers, and ChoicePoint may sometimes be a credit reporting agency or a credit bureau, and it may sometimes be covered by Gramm-Leach-Bliley for other reasons. But as Chairman Majoras has testified, they are not covered by Gramm-Leach-Bliley in all their businesses. They are essentially unregulated in the view of the consumer groups, and they should be regulated more like credit reporting agencies under a robust system than merely covered by the security rule known as the safeguards rule.

Senator DODD. Well, Mr. Chairman, I would invite us to maybe look at that as part of our——

Chairman SHELBY. I think that is a very important question.

Senator DODD. Let me move, if I can, to one other area. Again, I think you have all pointed out this is complicated. The freeze issue is one that is—because it is a double-edged sword, obviously. It is a benefit obviously to the consumer to be able to protect that credit information. The other side of that sword is, of course, that same consumer then who wants to get a credit card, wants to buy a home, wants to buy a car, wants to unfreeze that information or they are not going to get they are seeking or the products they may

be pursuing. And the industry says—and I hear you, and I am not suggesting it is simple. But this is a complicated matter to turn on and turn off.

I want you to walk me through this a little bit. We are in the 21st century now, and it seems to me we have—and, again, I am old enough now to find all of this terribly complicated, but I know there are people smart enough to figure this out. Why is it so complicated to do that? Why does that become so hard to do? And I realize it can be complicated, and you can go back and forth rather quickly. But today, given the technology that exists that allows us to be able to transfer trillions of dollars at the speed of light, it seems to me the ability to respond to the customers that we seek, whose business we enjoy, whose hard-earned dollars we take, we cannot do a better job of responding to those people today. I mean, 15 million people in 6 months in this country have been potentially subjected to identity theft, and the numbers are growing. And I do not quite understand—and I may be terribly naïve about this—why the industry with all of its sophistication cannot more sophisticatedly respond to that consumer who wants to be able to engage in that stop-and-go process. Tell me why that is difficult. Walk me through it. Do you want to start, Mr. Ireland?

Mr. IRELAND. Senator, I think you have to add an extra party to the transaction. Under what this Committee and the Congress did in the FACT Act, a consumer who thinks they are going to be a victim of identity theft can place an extended fraud alert on their file, and a creditor opening a new credit account has to talk to that consumer, either in person or call them on the phone, before they open the account to make sure that they are dealing with the right person. Now, that system is not infallible. It has been in effect since last December, but we think it is working and it is too early to give that up.

In the security freeze context, in order to go through with the transaction you have to add another party to the communication. The consumer has to talk not only to the prospective creditor but also to the credit bureau and authorize the credit bureau to release the information. And that all has to happen at the same time.

We do transfer trillions of dollars around the country by wire transfer, but those are over dedicated lines in very carefully constructed systems. And my ability to talk to the credit bureau from the lobby of an auto dealership when I want to buy a car, convince the credit bureau who I am, and then have them release the report back to the auto dealer so that the auto dealer can use the report to give me a loan is more complicated than my talking directly to the auto dealer and the auto dealer verifying who I am.

You might get there at some point in the future, but I think right now you have complicated the transaction. It is not just auto dealers. It is checkout lines at retail stores where they are going to offer you a discount for entering into a charge arrangement with them, and numerous other places. And that addition of another party creates another link of secure communications. You create a triangle instead of a bilateral relationship, and that is a challenge.

Senator DODD. Any distinction here you want to tell me for the life insurance industry or the securities industry?

Mr. SCHWARTZ. I think Mr. Ireland summarized it very well.

Senator DODD. It would be a similar situation where you are talking about a trilateral relationship with insurance?

Mr. SCHWARTZ. Well, somebody who would be applying for insurance would have to release the freeze, and then there would be a question as to how do you identify the person. So, I think you would run into the same potential for unintended consequences, and inefficiencies in terms of processing applications.

Senator DODD. Is the industry thinking about this at all and how to, in fact, do this? It seems to me it is a service that would be rather attractive in terms of who I do business with. If the insurance company I do business with offers this service to me to be able to respond to my desires to have that credit information available or not available to people, it would be a very attractive offer.

Mr. SCHWARTZ. That would have to be addressed on a company-by-company basis, Senator, and we would be glad to get back to you on that.

Mr. HAMMERMAN. The only thing I would add from the securities industry standpoint is that the industry, as you know, is heavily regulated, and there are times that the industry may need to tap into that credit report when the consumer has put a freeze on for the industry to comply with the USA PATRIOT Act or other obligations that it has. So that would just be something to look at. But obviously, being able to provide this tool to a customer undergoing the difficulties of identity theft is important.

Senator DODD. Do you want to comment on this?

Mr. MIERZWINSKI. Well, I will just say—and I will let Stuart have the last word for once after me—I think that fundamentally this is the first consumer protection in the privacy sphere that has really given consumers control over their information. And so there is a philosophical disconnect between the industry and the consumers. Really, a lot of our privacy laws are in name only. They allow the sharing of information as long as disclosure is made. Our industry has gotten used to a system where they are in the driver's seat all the time. This puts consumers in the driver's seat, and it is new, so it is going to take some time. But if you adopt it nationwide, I believe that they will make it easier for us because it will be in their interest to do so.

Mr. PRATT. Senator, from our perspective, we are obviously the one that has to effectuate the freeze. Let me just remind all of us, of course, of a few truths that we have.

This Committee and other Committees in the Congress and ultimately the USA PATRIOT Act Section 326 places obligations. That has been mentioned. It is important to know that that is out there and that companies must take additional steps to verify identities for those purposes, and that inures benefits to consumers even into the realm of risk of becoming a victim of identity theft.

Fraud alerts, Mr. Chairman, you have discussed this before, and fraud alerts are another flexible choice that you have offered consumers today. I can place a temporary alert while I am still trying to decide whether I really have a higher level of risk. If I am a victim, I can place an extended alert on my files. So those choices are out there today.

So there are many systems today, some of which are just brand new with the FACT Act, that are not final, that have not been test-

ed large-scale in the marketplace. And this is also somewhat true for file freezing, and I think that is important. File freezing we think of as being out there for some time. It has been in California's law for some time. But in California, we only have 9,000 consumers who have frozen their credit reports.

Senator DODD. I am sorry. What is that again?

Mr. PRATT. Nine thousand.

Senator DODD. Have what?

Mr. PRATT. Out of 25 million or more consumers who are credit active in California, only 9,000 have frozen their credit reports. So we have a hard time giving you a good granular answer as to does it work, does it not work, how do consumers feel about it, how often are they act the countertop. What has been described by Mr. Ireland is true, though. If a consumer is at the countertop, we still have the question: How do you close the transaction at that point? Do you want consumers blurting out PIN numbers, if you will, at the countertop to the clerk who is hired during the holiday season? And how secure is that?

You will have all the same kinds of challenges that you have in the online banking world where you have to authenticate consumers. To what extent do you have to deploy a two-factor authentication system to ensure that you are really unfreezing the file for the real consumer and that you do not at some point find that criminals, as has been pointed out, who get clever about these things start to chase you down the road a little bit further?

I do not want us to think of file freezing as a panacea that somehow definitely cures all the ills, and I think you said it very well, Senator. It is complex.

Our only message here is to say that in the absence of a dialogue here at the Federal level, and regardless, really, of what you do now or later, the States are continuing to act on this. And so our concern is variations of standards. We have some States beginning to say, well, you should be able to turn it on in X number of minutes. I cannot tell you what an anathema we think that is. We might as well just also obligate every credit vendor in the country to approve credit applications in X number of minutes, irrespective of whether the USA PATRIOT Act was complied with or not or irrespective of whether we have deployed all the fraud prevention tools or not. So those are concerns for us, that, in fact, we are now having on a service level performance standards.

To your point, we will over time, regardless of what the Congress does, have to live with some degree of file freezing in this country for some percentage of the population. I think it will grow next year as a result of legislative activity. And we will have to find a way to deploy a system that operates with the variations that we see in the States today.

Senator DODD. I see Senator Reed is here, and I have taken more time here, but I am just curious on the Katrina issue. I had asked, Jack, before you walked in, what has happened with that at all. Any comments you want to share with us about the victims here?

Mr. PRATT. Absolutely. We have three areas of focus with Katrina.

First of all, the nationwide credit reporting systems have each set up toll-free numbers, either dedicated or options for Katrina

victims specifically. Those toll-free numbers allow you access to live personnel up front because we know Katrina victims many times have left their homes with little or no information, little or no financial information that they really need in order to be properly identified. So, I think the human touch is very important in those cases.

All Katrina victims have access to free reports. *Annualcreditreport.com,* the website through which you can obtain free reports, one of the elements of the FACT Act that was brought forward by this very Committee has been opened up so that free reports are available to consumers who can be authenticated online. But the key here is that when you cannot for some reason, we will have live personnel try to work through with you how to get a credit report to you.

We have a lot of complexity. Are you still—you know, unfortunately, because of the new hurricane heading toward Houston, we now have a group of Katrina victims who are moving out of Houston and moving out of Galveston and some of the areas that are affected. So those addresses that might have been temporarily set up have now shifted again. And so the key is not to have credit reports floating, if you will, out there in the Postal Service at the same time. But we are dedicated to doing that.

Second, within the first week of this, we sent out communications to more than 16,500 data furnishers, more than 40,000 discrete contacts within the data furnisher system, notifying them of specific guidance on how to use the Metro–2 data format, the Metro format to report natural disaster as an annotation on your credit account. We also explained how you could report account deferrals. This was in support of Treasury Secretary Snow's advocating lenders take a lenient approach to all of this.

Third, though candidly I hope we never have to use it, we have now brought online a new Katrina dispute code so that if, in fact, at the end of the day, after all the communications to data furnishers, we have the unintended consequence of data reported that affects a consumer, we want to be able to sensitize that data furnisher very quickly to the fact that this is not just a dispute; this is a dispute about a victim of the Katrina disaster.

Senator DODD. Any evidence of identity theft at all occurring in the midst of all of this? It seems like a rather open system here, people calling in. I do not want to tie up the Committee time on this, but I am a little uneasy. Someone calls in and says they are so-and-so, give me my information.

Mr. PRATT. Rest assured, Senator, the fact that you have access to live personnel does not mean that we are going to automatically make the decision to turn that credit report over to the individual on the call. Protocols that we probably should not discuss in a public forum are deployed in order to test——

Senator DODD. I am curious only because it may apply exactly to what we are talking about here in the freeze information. If you have found a means by which you can confirm information for people who do not have their data that they left back in their homes in Louisiana or Mississippi, it might be an interesting process to give us some guidance on how to address these issues outside of a natural disaster circumstance.

Mr. PRATT. We do not know how easy that is going to be, by the way. This is new and uncharted territory. We are going to have to have these discussions with consumers along the way. Our hope is many of them can be authenticated through traditional systems so we do not actually have to move off point, if you will.

Senator DODD. I appreciate that.

Thank you, Mr. Chairman. I thank Senator Reed. I took a lot of time.

Chairman SHELBY. Senator Reed.

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

Thank you, gentlemen. We are faced with an issue that we inevitably confront when we are trying to craft legislation, particularly when there are competing State legislative schemes, and that is coming with a national standard that is adequate, not just a national standard that is there but does not provide protection. I know we have talked about the California standard.

And I am curious, I think Mr. Mierzwinski indicated that the California standard is something he sees as a good starting point, but I would like to get impressions of all the panelists about the California standard as a starting point for a national standard. One reason is it covers already a significant portion of the population. Is that an appropriate place to begin, particularly in terms of notification, or what things should be added or subtracted? Mr. Pratt?

Mr. PRATT. From our perspective, the basic operation of California is a standard that we apply generally, but I think that as has been discussed, California has what is called an acquisition standard for its notification trigger. And this is where we do digress from, I suppose, the support for a national standard for notices to consumers.

An example would be a laptop is stolen, a laptop is fenced, a laptop is recovered in a short period of time, and forensics indicates that nothing was done with that laptop. It was never even booted up. It was simply sold for cash, and the purpose for the crime was simply to get cash and not to use the data.

The California acquisition standard, on its face in the law, would still require that you send every consumer a notice saying that your information was breached, although we know technically it was not, meaning the forensic analysis would tell you otherwise.

So our only reason for pushing back on that is to make sure we do not send notices and create anxiety where anxiety is not necessary. What we want to do is make sure the notice is targeted to the risk, and I think this has been said several times on the Committee. Our goal and the goal that we will have to wrestle with is ultimately a goal the Committee has to wrestle with, is to make sure that we have the right trigger so that we send good, actionable notices, notices that consumers open, notices that consumers act on, and that is really the only underlying goal for why we push back on a sending notice to all consumers type of standard. We believe it has to do with remediation and taking actions when you are at risk.

Senator REED. Mr. Mierzwinski, can you tell me——

Mr. MIERZWINSKI. This is other than preemption the status of the harm trigger is where the consumer and privacy community

disagrees the most with the industry. Our view is you do not have an acquisition-based trigger, then you will not have companies doing a good job of protecting information in the first place. I would prefer that all those laptops have encrypted information on them, but then I hear that banks are losing laptops without even passwords, laptops let alone that are encrypted. So if you force the companies to disclose, there will be fewer losses, there will be better protection of the information.

And the second point I made earlier is that 50 percent of people do not know where their identity theft came from, and if they start getting notices, they start keeping those notices, and then they later become a victim of identity theft, they may be able to track it backward and more people will find out how they became victims if they receive more notices,

Senator REED. I do not want to necessarily retrace ground you have covered, but I am curious if Mr. Hammerman, Mr. Schwartz, and Mr. Ireland have comments. Mr. Hammerman.

Mr. HAMMERMAN. Thank you. As Mr. Pratt had mentioned, the difficult with the California standard is that being an acquisition standard, the result will be an over-notification, if you will, even though there is no substantial risk of harm of identity theft to the customer. For example, if someone misplaces their Blackberry, their hand-held device that might have a customer name and phone number, that does not necessarily mean that customer is at risk of identity theft or other account fraud. Yet, as I understand it, under the California standard, a notification would be triggered, and we think that is the wrong balance.

We think having the trigger apply when there is a significant risk of harm to the customer, that is the appropriate balance.

Senator REED. Let me inject one more point, which is, if the California standard is not adequate, what is the appropriate standard, from those people that would depart from that standard?

Mr. HAMMERMAN. From the securities industry standpoint, we would look forward to working with the SEC as a functional regulator to develop the details around the concept of significant risk of harm of identity theft or other fraud to the account.

Senator REED. Mr. Schwartz, Mr. Ireland.

Mr. SCHWARTZ. Senator Reed, actually, the California legislation just does not say "unauthorized acquisition" alone, it says "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the information." Those are ambiguous words that may very well impose or carry with it a standard of harm. I think the concern is the ambiguity and the fact that really you want to send a notice when there is a substantial likelihood of harm to consumers. So even the California legislation is not entirely clear as to what triggers a notification requirement.

Senator REED. Mr. Ireland.

Mr. IRELAND. I think I would agree with several of the other panelists, and Mr. Mierzwinski and I would probably disagree here. We are in favor of a risk-based standard. We think that California can be read to be an acquisition standard. Mr. Schwartz points out the compromise language, but it is not terribly clear what that means. We are concerned that California results in over-notification, and therefore it lessen the effectiveness of notices.

Senator REED. Mr. Pratt.

Mr. PRATT. Senator, just one last point. If you go to the California Office of Privacy, they provide additional guidance on what they think the acquisition standard means. That acquisition standard looks more like a harm standard, so it is very important to look at the California guidance that underlies the statutory regime that you have in California.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

Chairman SHELBY. Senator Carper, you have any comments?

STATEMENT OF SENATOR THOMAS R. CARPER

Senator CARPER. I just have a quick question. I apologize for missing the hearing. We were having a markup on Homeland Security on Katrina, and a number of bills that we are just still working on.

I want to ask maybe one question if I could of the panel, Mr. Chairman?

Chairman SHELBY. Go ahead.

Senator CARPER. First of all, thanks for being here and for your input. I understand that several States have enacted laws to protect the consumers against identity theft, and are now enacting laws mandating companies inform consumers when the consumer's information has somehow been compromised. I just want to ask which State approaches do you think work the best, if any, and why? We think of States as laboratories of democracy, and to see if there might be a model out there for us to emulate, and that is basically what I am asking you to help us do, identify if you think they are doing a particularly good job. No, not all at once.

[Laughter.]

Mr. IRELAND. Senator, the lag in responding to your question is that it is complicated. All the State laws differ, and there are good pieces in a law here and there and I think we can very much learn from the States, and much of the testimony that has been given here today has been based on experience with some of those State laws, particularly California.

I am not sure that I would advocate any particular State law as a single model. I think the issue of the way notification needs to be given and the factors it needs to address are perhaps more complicated and complex than many of the States have recognized, but we can certainly learn from those States.

We can also learn from some of the mistakes, because, for example, Illinois has a law that says there is no delay for law enforcement in notification, even though every other State has a law that provides for delay, so that the law enforcement people can go try to get the crooks. In the current situation, the Illinois law effectively nullifies all the rest of the delays in other States, because you give notice in Illinois and the cat is out of the bag.

I think the States have provided a valuable laboratory here and we can learn from each of the State laws, but I would not pick any particular one and make it the sole model to look to.

Senator CARPER. Do any of the other witnesses want to agree with anything that Mr. Ireland has said, or disagree?

Mr. SCHWARTZ. I would say, Senator Carper, that certainly the States do have provisions that we can look to, for example, for types of information that would be regarded as sensitive, personal information that would be the subject of the legislation, the various triggers, so I think there are elements in there, and I would agree with Mr. Ireland, that we should look to them and consider them and determine whether or not they should be applicable.

But in terms of coming up with a specific State that has the magic bullet, I do not think that there is one.

Senator CARPER. Thanks. Others, please?

Mr. HAMMERMAN. I would agree with what has previously been said.

Mr. MIERZWINSKI. Senator, the Consumer and Privacy Group testimony, Appendix 2, we list all the breach laws. Nine of them have no so-called "harm trigger," starting with California. We prefer laws without a harm trigger.

We also list in Appendix 3 all the State security freeze laws, and the best one is one that is expected to be signed today, which would be New Jersey's, because it makes it easy for consumers to selectively unfreeze their credit, and it is very inexpensive and it applies to all consumers. Those are the kinds of principles we believe in.

Senator CARPER. Thanks.

Mr. PRATT. From our perspective, we would again agree with Mr. Ireland in terms of the characterization. Carrying forward your laboratory analogy here, really, it is up to you to find a final precipitate to know what it is that should be mixed and workable for the entire country. We have great confidence you will be able to do that as you have done with many other Federal laws that have created national standards.

And as for file freezing, again, I think it is a dialogue that we really just would like to continue to have with all of you. We disagree with Mr. Mierzwinski about the merits of the New Jersey standard, in particular find it troubling because it creates regulatory powers at a State level over what is a nationwide credit reporting system. We think that that is the wrong direction in which for us to head.

Senator CARPER. One last quick question, if I could, just of Mr. Mierzwinski?

In recent years we have seen an increase in certainly in the awareness of identity theft and the steps that people can take to protect themselves. Do you think consumers have enough information about ways to guard against prior financial privacy? And if not, what if anything can we do on this Committee here in the Congress to further educate people that is not being done, and is there something else you can think of that the financial services industry should be doing themselves?

Mr. MIERZWINSKI. That is a big question in terms of identity theft and financial privacy. On financial privacy, I think the consumer groups are on the record. The Gramm-Leach-Bliley privacy notices, the problem with them is they are rights without remedies, and that is why consumers get frustrated. We need to give consumers privacy rights, not simply privacy notices.

In terms of identity theft, I think that consumers are starting to become more aware of the problem, but again, more information would always be adequate, and we will certainly think about ways that we can provide the Committee with greater recommendations to educate people about identity theft.

When you are a victim of identity theft and when you contact your credit bureau, they do send you information automatically, am I correct?

Mr. PRATT. That is right.

Mr. MIERZWINSKI. That is right. So at the point of contact with identity theft you find out about it. However, in advance of identity theft there needs to be better ways to find out.

We have been concerned that some of the companies are making money on identity theft, selling credit monitoring services. I would point out that this summer the Federal Trade Commission fined Experian, one of the big credit bureaus, $950,000, for deceiving consumers into obtaining its subscription based credit monitoring service, which it was marketing as if it were free. So we have to be careful how we urge companies to provide information.

Mr. PRATT. Senator, if I could?

Senator CARPER. Very briefly. I have used up all my time.

Mr. PRATT. We are mixing apples and oranges here. There was a marketing issue that was addressed by the Federal Trade Commission, the same Federal Trade Commission that said the monitoring services are a good idea. They do serve consumers. They are a product in the marketplace. It is like saying that home security systems are a bad idea, or OnStar in your car is a bad idea. Monitoring services are in the market because we have a great market and because we create great products in that marketplace, and monitoring services are one of those, and millions upon millions of consumers are purchasing them today.

Senator CARPER. Gentlemen, thank you all very much.

Mr. Chairman, thanks for giving me a chance to ask those questions.

Chairman SHELBY. Thank you, gentlemen. This is a very informative panel. This is a very complex issue, as we all know.

The hearing is adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]

[Prepared statements, response to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF MARK PRYOR

A U.S. SENATOR FROM THE STATE OF ARKANSAS

SEPTEMBER 22, 2005

Chairman Shelby, Ranking Member Sarbanes, and Members of the Banking Committee, I thank you for your kind invitation to testify about identity theft and security freeze.

As you are all aware, identity theft is one of the fastest growing financial crimes in the country. According to the Federal Trade Commission, almost 10 million people per year become the victims of identity theft. It is especially important to my constituents in Arkansas. Identity theft is in the top category of reported fraud in my State, with over 1,397 cases last year. It is an issue that I have cared about since my days as Arkansas Attorney General.

The Identity Theft Resource Center noted that identity theft victims spend on average about $1,500 and expend 600 hours of time to restore their credit histories after they realize what has happened to them. In addition, this crime costs American business an estimated $48 billion annually this must be prevented. A person's sensitive personal information is better than gold bullion. It weighs nothing, and in the hands of an experienced thief, yields far more wealth than the victim may actually possess. And all of our sensitive personal information is very vulnerable.

The California notification law educated every American consumer about the difficulties of keeping our sensitive personal information safe. Companies can lose it off a truck, accidently expose it, or have it stolen from them. It seemed that there was a large breach at every turn. First, there was ChoicePoint, then Lexis-Nexis, Card Systems, DSW, and the list goes on and on.

The goal is to make sure that companies adequately safeguard the personal information they keep. Then, in the event of a breach or a loss of sensitive personal information, we want to make sure those consumers are notified as soon as possible so that they can protect themselves from the potential identity theft.

The issue that struck me is that we are not providing consumers the tools to protect themselves. And we should give consumers a broad array of positive actions they can take to protect their information. An ounce of prevention is worth a pound of cure.

The Federal Government can place as many requirements as they please on businesses to protect sensitive personal information, but breaches will still happen. Hopefully, after a strong identity theft law is passed there will be fewer occurrences, but they will still happen. Sensitive personal information is readily available in paper sources and public records. Identity thieves will still steal mail and dig through trash for sensitive personal information.

As a quick example, my staff has received 11 prescreened credit offers at his home in the past week—several of them for previous occupants. It is this environment that spurred me to introduce S. 1336, The Consumer Identity Protection and Security Act of 2005, to provide the opportunity for consumers to have a choice to place a security freeze on their credit reports.

There is a philosophical tension regarding passage of a national security freeze law. Several States have security freeze laws in force right now, including California, Louisiana, Texas, Vermont, and Washington State, and even more States are considering such a law. Maine and Nevada security freeze laws are scheduled to come online in the next few months.

Usually, in this situation, businesses come to Congress looking for a national law for uniformity. This is the case in terms of the notice issue and safeguarding information, but not when it comes to providing security freezes.

I see the provision of a national security freeze law as the means of providing consumers a choice to protect themselves financially and to exercise their right to privacy. Security freezes are not for everyone. If a consumer enjoys having the ability to apply for instant credit and does not wish to surrender that convenience, he or she should not place a security freeze on their credit report. On the other hand, if you are a consumer that is not interested in instant credit and wants to eliminate the possibility of identity theft being turned into a tremendous financial loss, then a security freeze may be the right tool.

The constituencies that argue against security freezes make the argument that consumers are too accustomed to having instant credit, and that having security freezes available to all consumers will have unintended consequences, such as missing sales or missing offers with short time frames. Or more simply stated, they do not want to lose customers for instant credit.

But what is the danger in giving consumers a choice? The credit reporting agencies currently have to honor the security freeze laws for California, Louisiana,

Texas, Vermont, and Washington. The agencies will have to honor the security freeze laws of Colorado, Connecticut, Illinois, Maine, and Nevada, so impracticability is clearly not the issue.

There were 21 other States that considered security freeze legislation this year, with bills in New Jersey and North Carolina waiting for their governor's signature. In fact, technology companies in California are currently in the development stage of products for one-stop-shopping for consumers who wish to have their credit frozen at all three credit reporting agencies. In as little as 60 days, this type of one-stop-shopping for consumers could be available to all consumers in States where security freeze laws have been enacted.

People that elect to put a security freeze on their reports are not customers for instant credit, just like people who elect to put their names on the Do Not Call list are not customers for telemarketers. To not provide consumers this choice because they will not understand the inconvenience a freeze may cause them does not strike me as a reason to deny Americans this protection. If this is truly a concern, educating the consumer would solve that problem.

Another criticism I heard while we were discussing this issue was that security freeze legislation would impede necessary functions that rely on access to credit reports. After reviewing what the States have done, I am convinced that carefully crafted exceptions will insure that the flow of information needed for identity verification, fraud prevention, debt collection, government services, and the maintenance of prior business relationships will ensure those functions can continue in the normal course while fully protecting the consumer. California and Texas have had security freezes in place since 2003, and business continues to be conducted there with no incident.

Still, credit reports are legitimately needed for fraud protection, to collect current outstanding debts, and for the proof of identity. Any national security freeze bill has to maintain the ability for proper and necessary uses of credit report information.

Yet another criticism I heard was that a security freeze is the same as a fraud alert, which can be placed on a consumer s account from the recently passed FACTA. This is not true. Fraud alerts, while providing a level of security, are not as comprehensive as a freeze. Fraud alerts last only 90 days. In order to get an extended fraud alert, a consumer has to prove they have already been victimized by providing a police report or an affidavit. In addition, fraud alerts do not prohibit the release of a consumer's credit information from a consumer reporting agency. There is room for a security freeze option.

Consumers that wish to have more flexibility in having instant credit but want a level of protection can use the fraud alert. If a consumer wishes to deal with a level of inconvenience but wants certainty that no new credit will be issued from his or her credit report can elect to have a freeze.

In summary, Mr. Chairman and Senator Sarbanes, I believe that strengthening data safeguard and consumer breach notification requirements are important to help stop identity theft. But requiring businesses to better safeguard data and notify consumers of breaches are not the only answers. I believe we must also provide consumers with new tools to prevent identity theft. A national security freeze law will provide consumers with that additional tool.

Consumers will have a choice on whether to actively protect their credit through affirmative action or to trust credit reporting agencies, financial institutions, data brokers, and others to do it for them. This is an important choice.

The option of placing a security freeze on a consumer's credit file has proved to be a viable and workable one in several States across the country. It is my hope that the Congress will agree to give this choice to all consumers across the country to help prevent them from becoming victims of identity theft and protect their most important personal information.

I thank the Chairman, Senator Sarbanes, and the Members of the Committee for inviting me to give testimony on this issue that is very important to me and my constituents. Thank you.

PREPARED STATEMENT OF STUART K. PRATT

PRESIDENT AND CEO

CONSUMER DATA INDUSTRY ASSOCIATION

SEPTEMBER 22, 2005

Chairman Shelby, Senator Sarbanes, and Members of the Committee, thank you for this opportunity to appear before the Committee on Banking, Housing, and

Urban Affairs. For the record, I am Stuart Pratt, President and CEO for the Consumer Data Industry Association.

CDIA, as we are commonly known, is an international trade association representing approximately 250 consumer information companies that are the Nation's leading institutions in credit and mortgage reporting services, fraud prevention and risk management technologies, tenant and employment screening services, check fraud prevention and verification products, and collection services.

We commend you for holding this hearing on the financial services industry's responsibilities and role in preventing identity theft and protecting the sensitive financial information of their customers. You have asked the CDIA to provide input on a number of issues that have been raised in hearings and legislation this year and in doing so, let me begin with some comments on how the Fair Credit Reporting Act[1] as amended by the Fair and Accurate Credit Transactions Act (PL 108–159) has already contributed materially to the protection of consumers by establishing new duties for the industry and empowering consumers with important new rights. It bears noting that these new duties and rights are all the more effective and easy for consumers to use because they are uniform. We again thank you, Mr. Chairman, Senator Sarbanes, and the Committee for the successful effort to set these national standards which are necessary to ensure that all consumers continue to enjoy the benefits of a nationwide credit reporting system and ultimately a low-cost, competitive and creative credit marketplace which helps fuel our Nation's continued economic expansion.

FACT Act

By December 1, 2004, all FACT Act amendments made to the Fair Credit Reporting Act were effective. As of this date our members had brought online a series of nationwide practices which inure particular benefits to consumers who may have concerns about identity theft. These national standards include:

Fraud Alerts—These alerts were voluntarily established by our members in the mid-1990's. Our members have long believed that fraud alerts strike the right balance for consumers who wish to ensure that a lender is notified of their concerns about identity verification where they have already been or may become victims of the crime of identity theft. Consumers recognize that while these alerts can slow down credit approval processes, alerts do not stop a transaction and, thus, consumers can continue to actively seek out better financial products and services whenever they wish.

The FACT Act created two specific types of fraud alerts. Initial alerts stay on the consumer's report for a minimum of 90 days and will be placed on the report even when there is just a concern that a person might become a victim of identity theft. Creditors which receive this alert must take steps to form a reasonable basis that they have properly identified the consumer. Extended alerts are placed on the consumer's file when he/she presents an identity theft report. This alert remains on the consumer's file for a full 7 years and it may include contact information for a consumer which can be used as part of the identity verification process. Most important to the codification of our members' voluntary fraud-alert practice was that the FACT Act tied the presence of the alerts to specific duties for the recipients. This tying of the consumer reporting agency's duty to place such alerts with a corresponding duty for recipients to form a reasonable basis for identity verification had never previously been established and our members believe that this materially improves upon the fraud alert systems that previously existed.

Active Duty Alerts—Though similar to fraud alerts, active duty alerts may only be used by individuals who are serving in an active duty capacity for our armed services. These alerts remain on the service member's credit report for 12 months and, like fraud alerts, are tied to duties for recipients to take steps necessary to reasonably identify the identity of the applicant before approving the application.

Address Discrepancy Indicators—The FACT Act also established additional protections for consumers in transactions even where a fraud alert might not be involved. Specifically, the FCRA now requires that where a nationwide consumer reporting agency receives a request from a creditor for a credit report and finds that the address submitted by the creditor differs materially from the address on the consumer's credit report, it must indicate to the creditor that this difference exists. Thus, lenders have an additional red flag to consider in attempting to properly validate the identity of an applicant. It is important to note that changes in addresses are not necessarily a strong indication of fraud when one considers that approximately 40 million addresses change each year in this country. Nonetheless, the FACT Act ensured an appropriate focus on address discrepancies by all financial in-

[1] 15 U.S.C. 1681 *et seq.*

stitutions and this adds additional protection for consumers. While final regulations specifying what a recipient of an address discrepancy indicator must do with them are not completed, no doubt these indicators are being used by lenders today.

Identity Theft Reports—The FACT Act also defined the term "identity theft report." This definition was a key to ensuring that victims of identity theft could avail themselves of a number of rights under the law even if they were having trouble obtaining a traditional police report. The ultimate success of this new definition is in the balance struck by the rules which ensure that such reports can be readily accessed and used by all victims without creating a situation where the reports are hard to verify, misused, or easily forged.

Identity Theft Reports and Blocking Fraudulent Data—In year 2000, CDIA's national credit reporting agency members established a nationwide voluntary initiative for victims of identity theft which allowed them to submit a police report and request that fraudulent data be blocked in victims' reports. The FACT Act codified this initiative and expanded it by use of the new "identity theft report" definition. In enacting this national standard, Congress ensured that all victims received the same treatment and that fraudulent data would be removed from victims' reports.

Red Flag Guidelines—Beyond the specific provisions of law discussed above, Congress recognized the need to empower regulators to develop guidance for financial institutions which is intended to encourage the use and accelerate the adoption of a robust combination of technologies and business rules to further reduce the incidence of identity theft. These guidelines are still under development.

The fact that the provisions just discussed all operate as national standards bears repeating. The Congress was prescient in recognizing that fraud prevention and, in fact, regulation of a nationwide system of credit reporting and credit markets is best handled through uniform national standards. A series of State laws which impede the free flow of information across this country cannot possibly achieve the same benefit for all citizens wherever they may live. We applaud the Congress and the principal sponsors of the FACT Act for the necessary focus on the needs of consumers and identity theft victims through the establishment of national standards of practice.

In closing our discussion of national standards under FCRA, I am reminded of the fact that the FCRA itself remains the only law which directly regulates our members operating as consumer reporting agencies. The national standards reauthorized and established by the FACT Act were critical to our nationwide members and it remains vitally important that our members operating as consumer reporting agencies are regulated under this single set of national standards, law, and regulation.

Information Security and Consumer Notification

Beyond the FACT Act's many new protections and rights for consumers, the security of sensitive personal information held by nonfinancial institutions has been the focus of debate in a number of House and Senate Committees. In fact, this Committee was the first to hold hearings on breaches of sensitive personal information and ultimately there are two key themes on which to focus:

- Ensuring the security of sensitive personal information; and
- Sending consumers meaningful notices of a breach of sensitive personal information when there is a significant risk of identity theft.

Information security and requiring consumer notification if the loss of information poses a significant risk are not new areas of focus for this Committee, which has traditionally taken a leadership role on information policy. Most recently enactment of the Gramm-Leach-Bliley Act[2] (GLB), Title V included a requirement[3] that Federal agencies write regulations[4] for securing and protecting nonpublic personal information, including taking into consideration when a loss of such information should lead to consumer notification. The FTC published its final rule on May 23, 2002 and they became effective on May 23, 2003.[5]

The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft has expanded beyond the boundaries of financial institutions. It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a "financial institution."

---

[2] 15 U.S.C. 6801–6809 (Financial Privacy).
[3] See Section 501(b) of Title V, PL 106–102.
[4] See 15 U.S.C. 6801(b), 6805(b)(2).
[5] 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule.

Safeguarding Sensitive Personal Information—GLB's statutory framework for safeguarding sensitive personal information is equally well-suited to information safeguards for sensitive personal information held by any person not otherwise defined as a financial institution. Under this approach, the FTC would promulgate rules for any nonfinancial persons just as they did under GLB. To ensure that there is absolute regulatory continuity between the applicable provisions of GLB and rules therein and new information security standards and rules, financial institutions which are compliant with their obligations under GLB should be deemed in compliance with any new requirements. Any new standards for nonfinancial entities should be substantially similar to those required by the GLB safeguard rule.

Consumer Notification—Consumers should receive notices when their sensitive personal information is breached and there is a significant risk of identity theft. While there are many details which go into creating an effective notification requirement, a fundamental element is making sure that it does not result in either over-notification, or too few notices sent where there is a significant risk to the consumer.

We believe that the general guidance provided this year by FTC Chairman Majoras in her testimony before a number of Congressional Committees regarding the appropriate "trigger" for a notice is on point. That is that notices should be sent when there is a significant risk of harm. In our view, harm is best defined as significant risk of identity theft. A poorly structured trigger leads to over-notification, which erodes the effectiveness of each subsequent notice sent to a given consumer. If notices are not tied to events that truly pose significant risks they will be ignored by many consumers who may become anesthetized to the importance of them.

Further, consumer reporting agencies as defined under FCRA Section 603(p),[6] are affected by the volume of even legitimate breach notices (in addition to those that result from over-notification). The national systems' contact information is consistently listed in notices going to consumers. If you add up even just a few of the high-profile breaches which have taken place over the course of this year, it is easy to come up with tens of millions notices containing our members' contact information. Thus, we believe that when a breach results in more than 1,000 notices to consumers, the company that breached the sensitive personal information should:

- Notify each nationwide consumer reporting agency of this fact and provide the estimated number of notices to be sent;
- Notify each other consumer reporting agency whose contact information will be listed in the notice; and
- Confirm the contact information that should be used for each listed consumer reporting agency. Our members report that there have been times when incorrect telephone numbers have been listed on notices.

A well-reasoned national standard for information security for sensitive personal information, coupled with effective notices where such information is breached by a party can contribute materially to the reduction in risk for all consumers.

Credit Report/File Freeze

You have also asked us to provide background on and discuss our views of the trend in State laws often termed "credit report freeze," "file freeze," or "security freeze." First, it is important to clarify that a freeze is not a fraud alert as enacted by the FACT Act. It is also important to understand how a file freeze operates based on our experience with current State laws.

A fraud alert accompanies a credit report sent to a lender and as such, a lender is notified of the consumer's concern. With a fraud alert, the lender can still process the application, though it will take additional measures to ensure that a consumer is properly identified before doing so. In contrast, a file freeze empowers a consumer to request that a consumer reporting agency not provide the credit report for a "new business" transaction such as an application for credit and, thus, the transaction cannot be completed.

File freezes are not absolute and consumers can request that a freeze be lifted temporarily for a period of time (for example, for 30 days). Depending on when and in what manner the request is received, this temporary lift does not happen instantaneously and consumers have to remember to make their request for a temporary lifting of the freeze to the consumer reporting agency prior to making an application for credit.

All State laws and proposals allow consumer reporting agencies to charge a fee for placing or lifting a freeze (how and where fees are charged varies by State). Our members have viewed the right to charge a fee for the placement of a freeze and for each temporary lifting of a freeze as a matter of equity where such laws are en-

[6] The Fair Credit Reporting Act: 15 U.S.C. 1681 *et seq.*

acted. California agreed with this principal when it enacted the first law in the country. Throughout the FACT Act hearings, time and time again this Committee heard testimony regarding the value that the credit reporting system brings to individual consumers. Simply put, credit reports lower credit costs, by lowering risk. Credit reports empower consumers and lead to the robust credit economy that benefits all consumers.

In the past several months, Federal legislation has been introduced which would codify the right of consumers to freeze the release of their credit reports and/or certain additional sensitive information under certain circumstances. These measures are, S. 1408, introduced by Senator Gordon Smith on July 14, 2005 which was marked up and reported out of the Senate Commerce Committee on July 28, 2005, and S. 1336 introduced by Senator Mark Pryor on June 29, 2005 and referred to the Senate Commerce Committee.[7] On July 21, 2005, Senate Banking Committee Chairman Richard Shelby introduced a virtually identical measure as S. 1336.[8] That bill was referred to the Senate Banking Committee. The Federal measures follow significant state activity over the past several years in this area. Currently, twelve states have enacted file freeze laws (California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont, and Washington). Since 2003, all but approximately 10 States have had file freeze measures introduced and though some have rejected the concept, this past year 7 States enacted new law. It is expected that there will be significant State activity in this area in 2006. The State laws vary in terms of substantive scope and operational elements. The measures contain different standards in the following key areas: (1) the circumstances under which consumers may request a freeze; (2) the extent to which consumer reporting agencies are required to notify other CRA's or entities which report affected information; (3) the extent to which certain information is exempt from a freeze; (4) the timetables within which freezes must be imposed or removed; (5) whether there are limits on amounts that can be charged to freeze or unfreeze reports; (6) and, the scope of liability for violations of the freeze laws. Though some file freeze provisions of State laws have been effective for years, our experience with them remains very limited. For example, we estimate that just a little over 9,000 California consumers have made use of the file freeze. With a population of more than 25 million credit-active Americans, this population of frozen credit reports yields no useful information regarding the individual consumer experience. Most State laws are very recent enactments and, thus, we also have no experience with consumers moving in and out of States where the file can and cannot be frozen.

The merits of file freezing have been heatedly debated in many State legislative forums and in media. Some States have in fact rejected file freezes. The consumer reporting industry has often been quoted as expressing concerns that the rigidity of freezes, which operate in stark contrast to fraud alerts where transactions can continue under a "caution flag." However, it is our view that as the number of State law enactment climbs, disparate State law file freeze provisions will increasingly affect the seamless operation of our Nation's credit reporting system which the FACT Act sought to preserve through the reauthorization of existing and establishment of additional national standards. Thus, in the context of significant State legislative activity, an increasing numbers of State file freeze laws, and also a country where 40 million consumers' addresses change each year, with many consumers moving across State lines, we must continue to monitor the risks to our nationwide credit reporting system and engage in an ongoing Federal dialogue about how best to preserve the efficiency and economic benefits that were protected first by the enactment of the FACT Act.

---

[7] Note that file freezing is only one of a range of issues addressed in this bill.

[8] The following quote by Senator Shelby drawn from the *Congressional Record* explains the Senator's motivations for the introduction of this bill:

"Mr. President, I rise today to introduce the Consumer Identity Protection and Security Act. This legislation provides consumers the ability to place credit freezes on their credit reports. Mr. President, my sole intent in introducing this legislation is to address a jurisdictional question that has recently arisen with respect to the Fair Credit Reporting Act. I want to make sure that the referral precedent with respect to legislation that amends the Fair Credit Reporting Act, or touches upon the substance covered by that Act, is entirely clear. I believe the Parliamentarian's decision to refer this bill to the Senate Banking Committee establishes that there is no question in this regard and that this subject matter is definitively and singularly in the jurisdiction of the Senate Banking Committee."

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

all intents and purposes, buy and sell comprehensive consumer information for decision-making about consumers, just as the regulated credit bureaus do. Although since its first reported[5] debacle Choicepoint has extended modest rights to consumers, these rights are not industry-wide and not guaranteed.

-- We also learned in the Choicepoint breach that the sloppy practices of financial companies extend well past losing unencrypted data tapes in shipping, failing to supervise third party processors or failing to prevent employee theft or computer hacking. Choicepoint actually sold detailed records on 145,000 consumers to identity thieves posing as customers.

-- We also learned that while the Gramm-Leach-Bliley Act imposed modest data security requirements (the so-called Safeguards rule[6]) on a wide range of financial and related firms holding customer data, that two major industry sectors were inexplicably left out of its definitions. Not only does the law fail to cover data brokers, it fails to cover third-party processors and servicers. Third party processors include companies such as Cardsystems, which is notorious for having had the largest reported breach, so far, which affected some 40 million credit and debit card numbers. Of course, the banks, credit card associations and other financial firms that contract with these processors should bear legal culpability for their failure to adequately supervise compliance with their own contractual requirements.

RECOMMENDATIONS:

In this testimony we make detailed recommendations for possible Congressional action. Although this committee has not yet drafted its own committee bill, we will comment on and compare key aspects of bills proposed in other committees. We urge the committee and the Congress, if you act, to adhere to the principles and recommendations below.

We say, "if you act," because many of our organizations believe that the states are responding well and are concerned that if the Congress does act, it could do so in a way that permanently prevents further state privacy laws from being enacted. Such an outcome – despite a continuing wave of identity theft and fraud, occurring at the same time as firms continue to share and sell confidential consumer information in ways that were not even contemplated in 1999 when GLBA was enacted – would pose grave risks to consumer privacy and to ID theft prevention, and would neglect the strong lesson that good public policy leadership depends on both the states and the Congress.

A strong argument can be made that the states' privacy leadership is adequate and continuing. Indeed, even before the 20 new states enacted breach notice laws of their own, other state Attorneys General forced Choicepoint and others to honor California's notice requirements nationwide. In the detailed testimony below, we will provide numerous other examples of ways that the states have demonstrated privacy leadership and make the forceful argument that we have never had the so-called uniform credit system that the financial industry lobby claims, and that the nation has been the better for it.

Principles for Congress to respond to security breaches and other new privacy threats:

- Any new legislation should not preempt state authority to enact stronger privacy and identity theft laws. Let the states continue to lead and work together with the Congress to find solutions. A marketplace where a consumer can buy products from only one seller is not competitive, nor is a public policy marketplace of ideas which is restricted to Congress.
- We oppose the use of a so-called "harm trigger" in security breach notice proposals. Any data security breach notice legislation should not grant unnecessary and litigable discretion to the firms that lost data to make their own decision whether there is a "likely" or "reasonable" or even higher risk of misuse before notice is necessary. 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.
- Any federal security freeze legislation should be available to all consumers, not only to past victims, as industry has insisted on in a few states. The intent of the security freeze is to protect all consumers, not only those with a strike against them already. Again, any federal law should allow states to continue to innovate and improve their laws. The newest security freeze law, in New Jersey, for example, builds on earlier efforts and contains many pro-consumer provisions not included in earlier laws.
- Congress should extend the requirements of GLBA's Safeguards rule to data brokers and third party processors.
- For data brokers, however, that is a necessary but not a sufficient condition. Data brokers should also be subject to a robust Fair Information Practices (FIPs)-based regulatory regime that, among others, gives consumers the rights to know about their file, to look at and correct their file, and control its use.
- Congress should fix the FACT Act. Too many of its identity theft remediation rights derive from bars that are too high for consumers to climb over or that provide only limited aid.
- Failure by firms to comply with any privacy rules should give victims a private right of action, as well as other Fair Information Practices based rights.

Finally, the issues before the Congress are fundamentally issues of privacy, as well as of identity theft prevention and data security. It is incumbent upon the Congress to understand that your response to these security breaches must recognize that these problems cannot be solved by merely imposing some additional security safeguard and notice requirements. Until the Congress recognizes that consumers need stronger privacy rights that extend to controlling the use of, as well as the misuse of what has aptly been called their financial DNA, these problems will continue to increase. Notice is not enough to protect privacy. Consumers need privacy rights.

Detailed Discussion

(1) The States Have Always Been Leaders On Privacy Protection

U.S. privacy law has always relied on state leadership; further, that state leadership has not stifled the economy in any way. Instead, the state leadership has stimulated eventual federal action and served to protect consumers better.

In 2004, two of our organizations, U.S. PIRG and Consumers Union, proposed a model state law[7] to enhance privacy and identity theft protection. It includes sections on the security freeze, security breach notification, insurance credit scoring regulation and other provisions.

- By the end of 2005, at least 20 states will have enacted security breach notification laws. At least nine of these laws have no harm trigger. (See Appendix 2 for a list of states. The list details which states have triggers.)
- Twelve states have enacted security freeze legislation. The most recent of these laws, New Jersey's, is the most innovative.

But these latest examples exist along a continuum of state privacy leadership often then emulated by Congress or regulators. Here are some other examples:

- As many as forty states had already enacted "do not call lists" before the FTC acted in 2003 to establish a national list.
- Seven states enacted free credit report on request laws before Congress enacted one in the 2003 FACT Act.
- California was first to enact a credit scoring disclosure law in 2000, after the FTC in the 1990s first supported the reform, then reversed itself and opposed score disclosure. Congress closely mirrored that provision in 2003 in the FACT Act.
- Two states – Washington and California – granted consumers the right to obtain business records from firms where identity thieves used their names before Congress added this benefit in the FACT Act.
- While California is most famous for taking advantage of the Sarbanes amendment to the Gramm-Leach-Bliley Act of 1999 to enact landmark affiliate sharing privacy rules in 2003,[8] several other states already had enacted opt-in regimes for financial data sharing and those laws have not been preempted.[9] In addition, North Dakota citizens, by referendum, overturned a bank-supported law that had eliminated their pro-privacy law requiring an opt-in before third party sharing.[10]
- Over a dozen states had enacted laws requiring the truncation of credit card numbers on consumer receipts before the provision was made nationwide in the FACT Act.
- While the FACT Act includes a modest provision requiring firms to provide a one-time notice that they may make negative reports to credit bureaus, Colorado has a much more privacy-friendly law requiring the credit bureaus themselves to provide annual notices to any consumers who have had negative information added to their reports.
- States have also led in other areas. California and Massachusetts enacted check float laws before the 1987 Expedited Funds Availability Act. California had enacted "Schumer box" type legislation before the enactment of the 1988 Fair Credit and Charge Card Act.

(2) Consequences of Misuse of Personal Information

The consequences of the misuse of confidential personal information whether obtained through identity theft or a security breach-- are both economic and non-economic and begin but do not end with identity theft. It is important that any legislation recognize that "identity theft" is not the only negative outcome of security breaches.

Financial identity theft where a consumer's social security number is used to assume their identity and open accounts in their name -- is a serious crime that has become more common in recent years as we have delved further into the "information age." Similarly, breaches involving acquisition of credit or debit card numbers can result in massive consumer fraud. The problem can be especially difficult when a debit card theft results in a thief draining a consumer's checking account.[11]

According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions about $48 billion annually and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and may spend hundreds of hours to clear their credit reports. A new study by the Identity Theft Resource Center provides comprehensive details on the types of fraud that occur and on the amount of out-of-pocket expenses and time victims spend clearing their names.[12] The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

Security breaches can certainly lead to financial identity theft but also result in other crimes. Increasingly, according to the Privacy Rights Clearinghouse and the Identity Theft Resource Center, consumers are becoming victims of criminal identity theft, where their confidential information is used to assume their identity for criminal purposes.

Confidential consumer information can also be misused for stalking and for tracking down victims of domestic violence who've attempted to hide from their abusers. Data on a consumer's financial or medical history can also be used to publicly embarrass him or her.

Information stolen may be used to commit terrorism. As is well-documented, the 9/11 terrorists used ID theft to get credit cards, apartments, and rental cars. In at least one case, one male hijacker successfully used the Social Security Number of a long-dead New Jersey woman.

(3) Data Brokers Evade The Fair Credit Reporting Act. A Robust Regulatory Regime Is Needed

In 2005, breaches have occurred in banks and their affiliates, retailers, card processors, government agencies and universities. Yet, there are a number of factors that set the breaches occurring at Choicepoint and Lexis-Nexis, the two data brokers with reported breaches, apart. First, the firms are virtually unregulated.

The 1970 Fair Credit Reporting Act (FCRA) was the nation's first major privacy law. Despite its flaws, which make identity theft too easy and also enable mistakes in credit reports that lead to consumers paying too much for credit or even being denied credit, the FCRA is a robust law that gives consumers Fair Information Practices[13] based rights. For example, consumers have the

right to know about, inspect, dispute and correct their files. The FCRA requires purpose specificity before a report can be accessed.

Yet the data brokers, including Choicepoint and Lexis-Nexis, have designed their business models to evade the Fair Credit Reporting Act's protections. In a December 2004 complaint[14] to the FTC, EPIC points out that:

> Americans face a return to the pre-FCRA era if companies like ChoicePoint can amass dossiers on Americans without compliance with any regime of Fair Information Practices. That era was marked by unaccountable data companies that reported inaccurate, falsified, and irrelevant information on Americans, sometimes deliberately to drive up the prices of insurance or credit. …ChoicePoint sells a number of FCRA products in the employment screening, tenant screening, and criminal background check fields. But the company also sells two products, "AutoTrackXP" and "Customer Identification Programs" outside of the FCRA's protections. AutoTrackXP is a database of 17 billion records that includes Social Security Number, addresses, property and vehicle information, and other information (citations omitted).

In a separate proposal, EPIC's Chris Hoofnagle and law professor Daniel Solove explain how data brokers exploit flaws in several poorly written definitions in the FCRA:

> The FCRA applies to "any consumer reporting agency" that furnishes a "consumer report." The definition of "consumer reporting agency" is any person who "regularly engages" in collecting information about consumers "for the purpose of furnishing consumer reports to third parties." This definition turns on the meaning of "consumer report," which is the key term that defines the scope of the Act. Unfortunately, the FCRA has a poorly drafted definition of "consumer report" that has allowed some to unduly narrow the Act's coverage. The Act conditions the definition of "consumer report" on how the information is used. That is, a "consumer report" is any communication bearing on a consumer's character or general reputation *which is used for* credit evaluation, employment screening, insurance underwriting, or licensing. Although the FCRA was passed to limit the uses of personal information in evaluating people, a literal reading of its definition of "consumer report" makes the law inapplicable if information is used for an unauthorized purpose beyond those enumerated in the Act. One could argue, for instance, that a criminal using credit information for fraud has not triggered the FCRA because fraud is not an authorized use. These problems in the definition of "consumer report" have allowed data brokers to avoid being regulated by the FCRA.[15]

In 1997, the data brokers convinced the Federal Trade Commission to approve their proposed self-regulatory scheme, under the so-called Individual References Services Group (IRSG) Principles. The Lexis-Nexis Privacy Policy states that "The IRSG consulted with the FTC in formulating its principles and auditing measures, and the FTC approved these principles and audit measures.[16]" In its "Individual Reference Services: A Report to Congress," the FTC in October 1997 stated the following: "The Commission commends members of the IRSG Group for the commitment and concern they have shown in drafting and agreeing to comply with an innovative and far-reaching self-regulatory program.[17]"

While the IRSG is now apparently defunct, the data broker business grew and flourished under this lax FTC oversight. Again, according to Hoofnagle and Solove:

> In the absence of statutory regulation, data brokers have adopted self-regulatory rules known as the Individual Reference Services Group (IRSG) Principles. The Principles set forth a weak framework of protections, allowing companies to sell non-public personal information "without restriction" to "qualified subscribers," which includes law enforcement agencies. "Qualified subscribers" need only state a valid purpose for obtaining the information and agree to limit re-dissemination of information. Under IRSG, individuals can only opt-out of the sale of personal information to the "general public," but ChoicePoint does not consider its customers to be members of the general public. The IRSG Principles were carefully crafted in order to ensure maximum flexibility by commercial data brokers. They have failed to set forth a reasonable degree of protection for individuals, and in fact, it was while data brokers were operating under these principles that the major privacy breaches occurred.[18]

Further, it is useful to examine the scope of the data broker enterprises and question whether it is good public policy to leave them unregulated, when you consider their power over both the government and private sectors. Choicepoint, for example, is the largest information broker in the United States. The company has amassed more than 19 billion records and has acquired a large number of smaller companies that obtain everything from criminal history records and insurance claims to DNA databases. The private sector and increasingly government rely on the data provided by Choicepoint to determine whether Americans get home loans, are hired for jobs, obtain insurance, pass background checks, and qualify for government contracts.

Not only does Choicepoint operate without regulatory scrutiny, employment or credit or insurance decisions are often made based on mistakes in their database, as numerous stories and studies have pointed out. According to a recent report[19] by Privacy Activism based on a review of a small number of reports held by Choicepoint and a second data broker, Acxiom, "The majority of participants found errors in even the most basic biographical information: name, social security number, address and phone number (in 67% of Acxiom reports, 73% of ChoicePoint reports). Moreover, over 40% of participants did not receive their reports from Acxiom -- and the ones who did had to wait an average of three months from the time they requested their information until they received it." While the study from Privacy Activism is only a pilot based on a small sample, it suggests that there may be serious problems with data broker data.

The data brokers have unfortunately resurrected the Bart Simpson defense ("it's not my fault") used by the credit bureaus in the early 1990s to delay needed remedial legislation to improve their accuracy rates. In the 1990s, credit bureaus claimed that they merely reported what the creditors furnishing information to them provided. The data brokers claim that they simply report public record information and that any errors aren't their fault.

But what if they mix up two accurate public records and report them on the wrong consumer? Shouldn't data brokers have duties to ensure that their data are accurate, just as credit bureaus do? Doesn't it make sense to impose a FCRA-like regulatory structure on their business model?

The companies' reliance on public records brings up another matter the purpose of and availability of public records in the first place. The firms often claim that they have some sort of a "right" to aggregate and re-sell public records for whatever purpose that they want. After all, the records are public, they say. But originally, the records weren't aggregated for new uses by private third parties. They were simply used, for example, to determine if the government was assessing your house accurately, compared to how it assessed your neighbor's. Hoofnagle and Solove point out, "Public records are essential for effective oversight of government activities, but commercial data brokers have perverted this principled purpose, and now public records have become a tool of businesses and the government to watch individuals."

If the government is going to allow use of public records for all these secondary purposes, then it should grant public record subjects greater rights when the records are aggregated and sold for these secondary purposes by data brokers.

(4) Approaches to Fair Information Practices-based Regulation of Data Brokers.

We believe that S. 500 (Bill Nelson) and S. 768 (Schumer-Bill Nelson) offer reasonable Fair Information Practices-based approaches to regulating data brokers through FTC rulemaking. But it is critical that the Congress not delegate all authority to the FTC, which failed to regulate the brokers in 1997. Security breaches and the effects on consumers of the ongoing maintenance of files on most Americans by information brokers are issues too important to be delegated in full to any regulatory agency.

Hoofnagle and Solove, in their "Model Privacy Regime" describe the framework which any new law should be based on. In our view, data brokers are most like consumer reporting agencies (credit bureaus) and should be regulated by a strict FCRA-like privacy regime, rather than merely subjected to the very general Safeguards rule of the Gramm-Leach-Bliley Act.

Any federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness.

(5) We support a strong security breach notification law without any so-called harm trigger.

Our organizations believe that any federal notice-of-breach law should do the following:

• Cover paper and computerized data.
• Cover government and privately-held information.
• Should not except encrypted data, due to weaknesses in encryption technologies. Consumers need to know every time an unauthorized person has accessed his or her personal identifying information, such as last name, address or phone number plus a social security number, driver's license number, or account number, particularly if robust encryption is lacking or compromised. This information is enough to open new credit accounts.
• Should not except regulated entities, such as financial institutions covered by the bank regulator guidelines.[20]
• Should have no loopholes, sometimes called "safe harbors."

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Testimony of

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

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before Committee on Banking, Housing and Urban Affairs
The Honorable Richard Shelby, Chairman
United States Senate

Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft

---

22 September 2005

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

Chairman Shelby, Senator Sarbanes and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations:[1] Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Consultant Mari Frank, Privacy Rights Clearinghouse, Privacy Times and World Privacy Forum.

Thank you for the opportunity to testify before you on the important matter of data security, data breach notices, privacy and identity theft. All of these organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. In particular, we commend you, Chairman Shelby, a founding member of the bi-partisan, bi-cameral Congressional Privacy Caucus, and ranking member Sarbanes, chief sponsor of the key privacy amendment to the Gramm-Leach-Bliley Act (GLBA) of 1999, which allowed states to enact stronger financial privacy laws.[2]

SUMMARY:

There are numerous lessons to be learned from 2005, a year when more than 75 reported data security breaches at some of the nation's largest financial companies, including Citigroup and Bank of America, as well as at other data collectors, have threatened the privacy and financial security of over 50 million Americans (see Appendix 1 for a list of breaches compiled by Privacy Rights Clearinghouse).

-- We wouldn't even know about these data security breaches if it weren't for the pioneering efforts of California, which enacted the nation's first security breach notice law in 2003. Pressure from other state attorneys general forced Choicepoint, then others, to comply with California's law nationwide. In 2005 alone, at least 20 more states have enacted similar breach notice laws (and one more expected to be signed), demonstrating that the states have the capacity to respond quickly to privacy problems and deserve to retain that authority (see Appendix 2 for a list of states enacting breach notice laws).

-- Buttressing this finding of state leadership, we have learned that the Congress acted wisely in 2003 when it chose to allow states to continue to enact stronger identity theft laws. While all of our organizations were gravely disappointed that the Congress chose to shut down many other state privacy initiatives with passage of the Fair and Accurate Credit Transactions Act[3] (FACT Act) amendments to the 1970 Fair Credit Reporting Act[4] (FCRA), it allowed additional identity theft policymaking by the states. Already this year, 8 states have joined California, Texas, Louisiana and Vermont in providing either victims, or better, all their citizens, with the powerful and innovative security freeze right to stop future identity theft. New Jersey's freeze (and breach notice) law is expected to be signed today. If you freeze access to your credit report for new creditors, identity thieves are left frozen, out in the cold (see Appendix 3 for a list of states enacting security freeze laws).

-- With the breach at the massive data broker Choicepoint, we learned that there is a massive and largely unregulated industry buying and selling astonishingly detailed dossiers on American consumers to businesses, private detectives and government agencies. The data broker business models are designed to carefully avoid regulatory oversight. The consumers who are their data subjects have virtually no privacy rights under law, even though the data brokers, for

PREPARED STATEMENT OF IRA D. HAMMERMAN

SENIOR VICE PRESIDENT AND GENERAL COUNSEL
SECURITIES INDUSTRY ASSOCIATION

SEPTEMBER 22, 2005

The Securities Industry Association[1] (SIA) welcomes the opportunity to testify concerning the financial services industry's responsibility to prevent identity theft and to protect the sensitive financial information of its customers. Maintaining the trust and confidence of our customers is the bedrock of our industry. The long-term success of our markets depends on customers feeling confident that their personal information is secure, and we therefore devote enormous time and resources to the protection of customer data. We are, however, concerned that the expanding patchwork of State—and local—laws affecting data security and notice will make effective compliance very difficult for us and equally confusing for consumers.

Data security and notice is the legacy of precedents set by the passage, in 1999, of the Gramm-Leach-Bliley Act (GLB), which this Committee was so instrumental in passing. We therefore applaud your leadership, Chairman Shelby, and that of Senator Sarbanes, in holding this hearing today. We are pleased that your Committee, given its breadth of understanding of the financial services industry, is actively reviewing these important data security issues.

As you know, at least four other Congressional Committees—the Senate Commerce Committee, the Senate Judiciary Committee, the House Financial Services Committee, and the House Energy and Commerce Committee—are currently actively involved in drafting legislation addressing many of these same issues, each with the intent to move their bills to the floor.

We are hopeful that, as a result of the review you and your colleagues are embarking upon today, you will agree with the conclusion that we and many others have reached—that the problem of data security, especially in this unique time, is a distinct Federal responsibility that requires a targeted Federal legislative and regulatory response. In light of the increasing number of disparate Federal and State legislative proposals, we urge this Committee to strike the appropriate balance that addresses both the concerns of American consumers threatened by identity theft and the duty of those of us in the financial services industry to provide meaningful protections.

Since 1999, SIA, through its member firm committees and working groups, has addressed the issues surrounding the protection of consumer financial information. During this period, SIA representatives have engaged in a dialogue with the Securities and Exchange Commission (SEC) staff to discuss the industry's requirements under the privacy provisions of GLB, including obligations to secure sensitive consumer information. In this regard, an SIA committee, comprised of representatives from 18 broker-dealers, meets regularly to discuss and focus on issues relating to the use, sharing, safeguarding, and disposal of personal customer information.

SIA and its membership have identified six fundamental principles that we hope this Committee will consider in drafting data breach legislation. Before turning to them, however, we wish to underscore our considered view that all businesses that have custody of sensitive personal information have a responsibility to provide data security measures commensurate with the sensitivity and nature of the data, and to notify consumers whenever a breach of security creates a significant risk of identity theft to the consumer. All businesses should protect the information that consumers provide to them, and justify the trust those consumers place in them by doing so.

Federal legislation addressing these duties must be carefully targeted to ensure that it is meaningful and can be speedily enacted. Legislation that extends beyond data breach, possibly into unrelated areas of privacy, will inevitably slow down the legislative process and delay, if not lessen, the chances for a prompt and appropriate Congressional response.

---

[1] The Securities Industry Association brings together the shared interests of approximately 600 securities firms to accomplish common goals. SIA's primary mission is to build and maintain public trust and confidence in the securities markets. SIA members (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. According to the Bureau of Labor Statistics, the U.S. securities industry employs nearly 800,000 individuals, and its personnel manage the accounts of nearly 93 million investors directly and indirectly through corporate, thrift, and pension plans. In 2004, the industry generated $236.7 billion in domestic revenue and an estimated $340 billion in global revenues. (More information about SIA is available at: *www.sia.com.*)

Overview

As the Committee is well aware, Section 502(b) of GLB generally prohibits financial institutions from disclosing "nonpublic personal information" to nonaffiliated third parties without first providing those consumers with an opportunity to "opt out" of such a disclosure. In addition, and even more relevant to the issues being addressed here today, Section 501(b) of GLB specifically requires financial institutions to implement appropriate "administrative, technical, and physical safeguards" designed to protect the security and integrity of their customer information. Congress fully recognized the inherent obligation of financial institutions to protect consumer information when it drafted Title V. To that end, and pursuant to GLB, on June 22, 2000, Regulation S-P was issued by the SEC.[2] This regulation requires every broker-dealer, investment company, and investment adviser registered with the SEC to adopt written policies and procedures designed to institute administrative, technical, and physical safeguards for information pertaining to sensitive customer records and information. In addition, broker-dealers are subject to periodic examination by the SEC and Self Regulatory Organizations for compliance with Regulation S-P.

Earlier this year, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and the Board of Governors of the Federal Reserve System collectively issued interagency guidance, again pursuant to Title V of the GLB, which sets forth certain affirmative obligations aimed at protecting sensitive financial information and notifying customers in the event of a security breach (Interagency Guidance).[3]

As the functional regulator for the broker-dealer industry, the SEC is similarly well-situated to issue guidance for broker-dealers, and SIA looks forward to working with this Committee, SEC Chairman Cox, and the SEC staff in determining how best to construct a notification regime that considers the likely effect of notification thresholds currently in effect in various State data security breach notification statutes. Specifically, as we discuss in more detail below, we would urge that the Committee consider a standard that links an obligation to notify consumers in the event of a breach with the crime of identity theft. We are concerned that any notification threshold that the Committee might consider for application to the broker-dealer industry should be tied to an actual threat to the consumer to which he or she might reasonably and effectively be expected to respond, and we believe that functional regulators (like the SEC) are best-suited to monitor how industry conforms to statutory requirements.

In considering legislation relating to data breach, SIA believes that the Committee should create a statutory framework under which regulations can properly and effectively be promulgated. In doing so, we urge the Committee to consider the following six principles:

- a clear national standard to achieve a uniform, consistent approach that meets consumer expectations;
- trigger for consumer notice tied to significant risk of harm or injury that might result in identity theft;
- a precise definition of sensitive personal information tied to the risk of identity theft;
- exclusive functional regulator oversight and rulemaking authority;
- flexible notification provisions; and
- reasonable administrative compliance obligations.

Principles for Legislation

Uniform National Standards

As of this morning, a total of 19 States—and one major metropolitan area, New York City—have passed security breach notification laws, and a number of other States are poised to consider legislation in this area. Very few States provide exceptions to coverage for functionally regulated entities at the Federal level. Although much of the early legislation enacted in the States was modeled after California's 2002 security breach notification law, which was the first in the Nation, States are increasingly enacting much broader legislation that differs in many respects from the original California law.[4]

---

[2] 17 CFR Part 48.

[3] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736–54 (Mar. 29, 2005).

[4] The California legislation, S.B. 1386, was enacted in 2002 and went into effect on July 1, 2003.

For example, New York City enacted three laws in May, marking the first instance of a locality enacting an ordinance placing affirmative obligations on businesses to safeguard data, dispose of it in a secure manner, and notify consumers in the event of a security breach. In addition, New York City also authorized the Commissioner of the New York City Department of Consumer Affairs to "refuse to issue or renew" any business license to any New York City business applicant or licensee if there are, among other things, "two or more criminal convictions within a 2-year period of any employees or associates of the applicant or licensee for acts of identity theft or unlawful possession of personal identification information." Additionally, any licensed business must "immediately notify the department upon the occurrence" of a judgment or conviction against any employee, or the business itself, of any one of several enumerated offenses. These laws all went into effect 3 days ago, on September 19, 2005.

Although some of these New York City provisions will likely be preempted by the recently enacted New York State data security breach bill, the provisions authorizing the denial of business licenses may not be preempted due to the construction of the preemption clause in the New York State legislation. The clear implication to regional and national businesses of this law is that, potentially, 100,000 or more localities in the United States may similarly decide to seek passage of their own data security compliance regimes, further complicating the compliance obligations of businesses that operate in more than one locality across the Nation. To this point, apart from the California and New York legislation, no other State has specifically incorporated provisions into their legislation preempting local branches of government within their States from instituting their own data security legislation.

From a policy perspective, a patchwork of 19 (and likely more) State laws, let alone those of potentially thousands of localities, does not and will not serve the public interest. In fact, the multiplication of State and local laws is likely to exacerbate the confusion and potential harm to consumers. Consumers in different States would be subject to different security standards and levels of notification despite the fact that the harm they may suffer as a result of a security breach at the same institution is identical. Additionally, businesses would be subject to such an array of obligations, which would be ever-shifting, that they may not be able to comply in one jurisdiction without running afoul of the obligations imposed on them in another.

For these reasons, SIA strongly urges that this Committee act quickly to create and obtain passage by Congress of legislation that results in a uniform national standard without subjecting the industry to a myriad of conflicting State and local laws.

Harm/Injury Trigger For Notice

A principal benefit to uniform national standards is the creation of a consistent definition for a trigger that results in the notification of consumers in the event of security breaches. SIA recommends that the Committee create a statutory framework that defines a reasonable and balanced notification trigger to be activated following a breach of security. Specifically, consumers must be notified when there is a "significant risk" that they will become victims of identity theft.

Under the California breach notification law, for example, the unauthorized acquisition of sensitive information—regardless of whether any harm has or could result from its acquisition—creates an obligation for the custodian of that data to notify consumers that it has been so acquired. The Interagency Guidance issued this year proposed that consumer notifications be issued whenever it was reasonable to expect that the data would be misused in a manner creating substantial harm or inconvenience to a consumer.[5] Of course, companies are always free to unilaterally issue notifications whenever they feel it is appropriate to do so. However, a Federal mandate should be linked to some demonstrable risk of harm to the consumer, such as the possible theft of the consumer's identity. Notification in the wake of each incident of data breach, without regard to significant risk of identity theft that might result, could well have the counterproductive effect of overwhelming customers with notices that bear no relation to significant risk, and therefore might not only needlessly frighten and confuse people, but also likely desensitize them to future notices altogether.

[5] In testimony before the Senate Commerce Committee this past June, Federal Trade Commission (FTC) Chairman Deborah Majoras observed that neither the "unauthorized acquisition" standard of California law nor the "misuse" standard of the Interagency Guidance is optimal. Instead, she and her colleagues on the FTC suggested a different standard, one in which notifications would automatically go to customers when a significant risk of harm to them exists as a result of the breach. See Prepared Statement of the FTC before the Committee on Commerce, Science, and Transportation on Data Breaches and Identity Theft (June 16, 2005).

Linking the notice trigger to a significant risk of harm strikes the appropriate balance for both consumers and financial institutions alike. Specifically, before a broker-dealer is required to notify potentially great numbers of customers of a security breach, it should be obligated to make a determination, following a reasonable investigation, that a significant risk of identity theft has occurred or could occur as a result of the breach. SIA recommends that the actual formulation for the notification trigger should be determined by functional regulators, through rulemaking. In the case of broker-dealers, the SEC is in the best position to make that determination.

Precise Definition of Sensitive Personal Information

As noted previously, 19 States and one locality have already passed laws imposing consumer notification requirements in the event of a security breach. In many of these States, the scope of the information covered by the laws varies widely. For example, Arkansas and Delaware have expanded California's definition of "personal information" to include medical information, while the definitions in the Illinois and Maine statutes include account numbers, regardless of whether they are accompanied by the security code required to access the account.

New York State's recently enacted law expands the definition of covered personal information even further, to include "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person," when acquired in combination with a Social Security number, driver's license or State identification number, or account number with a password or access code. Additionally, New York City's ordinance covers all forms of data, whether on paper or computerized, and whether encrypted or not. In addition, the North Carolina legislature unanimously passed a law just last month, which now awaits only the governor's signature, that would specifically cover "personal information in any form (whether computerized, paper, or otherwise)." This raises a question as to whether oral statements containing personal information are also covered by the impending North Carolina data security and notification law.

SIA believes that the scope of the type of information that underpins any notification obligation should be carefully defined so that the obligation to notify only arises when the sensitive personal information acquired in the breach can actually be used to perpetrate the crime of identity theft upon a consumer. For instance, in the absence of a key, encrypted information is useless to others who acquire it and should be excluded from the definition of sensitive personal information, as it was in the California law. Consumers would benefit more from a specific definition of covered personal information which includes combinations of identifying data, as opposed to a broad definition that includes any single piece of information which could not alone be used to steal a consumer's identity.

Exclusive Functional Regulator Oversight and Rulemaking Authority

Given the existing regulatory framework of GLB and the depth of expertise of the functional regulators in dealing with issues like identity theft and data security, any legislation should continue to recognize the primary role of the functional regulators in addressing these issues by granting them exclusive rulemaking and oversight authority.

Functional regulators are in the best position to evaluate the risks for consumers served by each sector of the financial services industry and to determine the specific consumer protection measures that best address them. Functional regulators also have the expertise to adjust these protections over time as threat levels change and the industry's ability to respond evolves. Likewise, functional regulators have the ability to examine the institutions they regulate for compliance and sanction those not in compliance. Accordingly, legislation addressing the security of data held by securities firms and other financial institutions subject to GLB should provide that the functional regulators of these institutions have the exclusive authority to develop and enforce appropriate regulations.

Flexible Notification

The number and variety of security breaches reported in the press over the past 8 months have made clear that the optimal means of notification will vary with the type and scope of security breach.

Accordingly, SIA suggests that businesses should be permitted to deliver the customer notice in any timely manner designed to ensure that a customer can be reasonably expected to receive it. The specific requirements of any notification process should be determined by the functional regulators whose unique expertise will allow them to determine the optimal means of notification.

Reasonable Compliance Obligations

Security breaches may occur through no fault of the business and despite the existence of reasonable safeguarding measures. As Deborah Majoras, Chairman of the FTC, said when she testified before the Senate Commerce Committee this past June, "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." When that happens, businesses should be permitted to raise as an affirmative defense that they have acted in good faith and implemented systems to reasonably comply with applicable regulations. This opportunity will create incentives for businesses to better secure data and reward those who have already taken such steps.

SIA supports a compliance regime that is both reasonable and predictable, with appropriate administrative liability for those businesses that fail to take the appropriate measures to protect sensitive consumer information. Given the complexity of the issues surrounding a data breach, and the intimate knowledge that functional regulators have about the financial services industry, SIA believes that any bill the Committee drafts should provide for administrative enforcement only.

Conclusion

American consumers and industries are currently facing a major threat from criminals, including potential terrorists, who seek to perpetrate identity theft. The financial services industry takes very seriously its duty to safeguard the sensitive financial information that pertains to its customers. The damage created by incidents of identity theft and other kinds of fraud are not only attacks on consumers, but also of serious concern to businesses whose reputations inevitably suffer from security breaches and who must bear the cost of the fraud in both lost customers and reduced confidence in their brand.

We believe that to resolve these issues, the Banking Committee should work to create carefully targeted legislation that embodies the principles we have outlined above. SIA is eager to serve as a valued resource for the Committee in this endeavor, and welcomes the opportunity to work with the Committee and its staff as it continues this critically important work.

Mr. Chairman, thank you again for the opportunity to testify before the Banking Committee today. I welcome your questions, and those of your colleagues, and will endeavor to answer them fully and completely.

PREPARED STATEMENT OF GILBERT T. SCHWARTZ

PARTNER, SCHWARTZ & BALLEN LLP

ON BEHALF OF THE

AMERICAN COUNCIL OF LIFE INSURERS

SEPTEMBER 22, 2005

Introduction

Chairman Shelby, Ranking Member Sarbanes, and Members of the Committee, I am Gilbert Schwartz, Partner in the Washington DC law firm of Schwartz & Ballen LLP. I am appearing before the Committee today on behalf of the American Council of Life Insurers (ACLI) to discuss the life insurance industry's responsibilities and role in preventing identity theft and protecting sensitive financial information.

ACLI is the principal trade association for the Nation's life insurance industry. ACLI's 356 member companies account for 80 percent of the life insurance industry's total assets in the United States. ACLI member companies offer life insurance, annuities, pensions, long-term care insurance, disability income insurance, reinsurance, and other retirement and financial protection products.

This hearing represents another chapter in this Committee's long-standing commitment to the protection of consumer information and to the prevention of identity theft, as evidenced by the Committee's central role in the enactment of the Gramm-Leach-Bliley Act (the GLB Act) and the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act). ACLI appreciates the opportunity to discuss with the Committee the important role that life insurers play in protecting sensitive financial information of our policyholders and in preventing identity theft.

Background

The issue of preserving the confidentiality and security of customer information is a critically important matter for our country. It is significant not only to the Nation's economic well-being, but also to insurers and other financial institutions that

use this information to provide vital services to our country's consumers. Due to the inherent nature of the life insurance business, ACLI member companies obtain and maintain sensitive personal information about their policyholders and insureds. The life insurance industry has long recognized the importance of maintaining and protecting the confidentiality and security of this information and ensuring that it is not otherwise compromised.

Life insurers have long been committed to establishing and maintaining processes that protect sensitive customer information and to preventing misuse of such information. Insurers expend considerable resources to achieve these objectives. They recognize that policyholders expect insurers to protect their confidential personal information. Life insurers' recognition of the need to protect customer information predates enactment of the GLB Act. Indeed, ACLI and its members were, and continue to be, strong supporters of Title V's privacy provisions.

The Gramm-Leach-Bliley Act

Title V of the GLB Act sets forth the Congressional policy that every financial institution has an affirmative and continuing obligation to protect the security and confidentiality of personal information of its customers. The institution's primary supervisor is required to establish appropriate safeguards relating to administrative, technical and physical safeguards to ensure the security and confidentiality of such information, to protect against anticipated threats or hazards to the security or integrity of the information and to protect against unauthorized access to, or use of, such records that could result in substantial harm or inconvenience to customers.

The Federal agencies with supervisory authority over financial institutions have adopted comprehensive guidance or rules implementing the GLB Act's data security provisions.[1] In addition, 34 States have adopted comprehensive regulations or statutes which establish standards for safeguarding customer information by insurers. The State requirements generally track the National Association of Insurance Commissioners' Standards for Safeguarding Customer Information Model Regulation and are consistent with the Federal guidance.

Under State law and regulation, life insurers are required to implement a comprehensive written security program that includes administrative, technical, and physical safeguards for the protection of customer information. The program must be appropriate to the size and complexity of the insurer and to the nature and scope of its activities. The program must also be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to customers. Insurers also require that companies from which they receive operational services maintain rigorous information security programs that meet the requirements of the GLB Act.

Identity Theft and the FACT Act

Consumers are very concerned with the issue of identity theft. The Federal Trade Commission has reported that the number of identity theft complaints rose to almost 250,000 in 2004, an increase of 15 percent from 2003. Identity theft accounted for 39 percent of the total number of consumer complaints, topping the list of consumer frauds reported by the Federal Trade Commission by an overwhelming margin.[2]

Congress enacted the FACT Act, in part, to respond to the growing crime of identity theft. It directs Federal regulators to develop guidance to identify and prevent identity theft. The Federal agencies have proposed and adopted several regulations and provided guidance to deter identity theft. We anticipate that additional guidance will be forthcoming to educate consumers and the financial industry as to how to reduce the incidence of identify theft.

Breach of Security Notices

As a result of growing concerns with the possibility of identity theft resulting from security breaches of information systems, 20 States have enacted legislation requiring companies to notify consumers in the event their sensitive personal information is affected by a security breach of their information systems. Additional States are considering legislation as well. These statutes typically require disclosure of a

---

[1] *See* 66 *Fed. Reg.* 8615 (February 1, 2001) (Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation, and Office of Thrift Supervision); 66 *Fed. Reg.* 8152 (January 30, 2001) (National Credit Union Administration); and 67 *Fed. Reg.* 36484 (May 23, 2002) (Federal Trade Commission).

[2] "National and State Trends in Fraud & Identity Theft, January-December 2004," Federal TradeCommission, February 1, 2005.

breach of security of the computer system to the person whose unencrypted sensitive information was or is reasonably believed to have been compromised. Generally, notice is not required if after reasonable investigation it is determined that there is no reasonable likelihood of harm to customers.

Some States have adopted requirements that differ in certain key respects. The need to track these differences and factor them into a notification program will inevitably make it more difficult for institutions to send notices to consumers promptly. The complexity resulting from differing State requirements will likely mean that consumers may experience delays in receiving timely notices. Moreover, State laws may also result in overlapping enforcement mechanisms, which increases the likelihood of uneven enforcement policies from State to State.

Federal Banking Agency Guidance

In March, 2005, the Federal banking agencies amended their interagency guidance on information security safeguards to require banking organizations to adopt response programs in the event of unauthorized access to customer information.[3] Under the agency guidance, depository institutions are required to develop and implement risk-based response programs to address incidents of unauthorized access to customer information in customer information systems. The guidance requires that if, after conducting a reasonable investigation, a depository institution determines that misuse of sensitive customer information has occurred or is reasonably possible, it should notify the customer as soon as possible. Customer notice may be delayed if law enforcement authorities request a delay so as not to interfere with their criminal investigation.

The notification requirement focuses on sensitive customer information because this type of information is most likely to be misused by identity thieves. Sensitive customer information is regarded as the customer's name, address or telephone number in conjunction with a Social Security number, driver's license number, credit or debit card account number, or password or PIN that would allow someone to access the customer's account.

Possible Federal Legislation

Uniform Nationwide Protections

ACLI supports Federal legislation that provides uniform national standards for notification to individuals whose personal information has been subject to a security breach. ACLI member companies believe it critical that the substantive requirements of Federal security breach notification legislation preempt State or local laws or regulations addressing any aspect of this subject matter.

When a security breach occurs, it is important that the institution that maintained the sensitive information move quickly to investigate the nature of the breach, determine the likelihood that information may have been misused and notify customers. The proliferation of State laws that impose similar but varying requirements could result in a delay in notifying consumers while separate notices are developed for consumers who are located in States with nonuniform standards. Varying State requirements, therefore, could have an adverse effect on consumers and increase the likelihood that consumers will be victimized by identity thieves. Accordingly, ACLI urges Congress to establish uniform preemptive guidelines that will apply nationwide. Such an approach will be beneficial to consumers because it will ensure that consumers receive the same information in a timely fashion regardless of where they reside.

Sensitive Consumer Information

ACLI believes that the Federal banking agencies and the States are correct in focusing attention on notice to consumers in connection with breaches of security of unencrypted or unsecured sensitive consumer information, such as a person's name and address when combined with such information as account number or Social Security number. While databases may contain other personal information about their customers, much of the information is of little or no value to identity thieves. Accordingly, ACLI recommends that security breach legislation apply only to sensitive consumer information obtained by an unauthorized person if the information is not encrypted or secured by a method that renders the information unreadable or unusable.

ACLI also believes that it is important that Federal security breach notification legislation apply to all businesses that maintain sensitive consumer information. Consumers should be protected regardless of the nature of the business that maintains their sensitive information.

---

[3] 70 *Fed. Reg.* 15736 (March 29, 2005).

Likelihood of Harm

ACLI member companies support legislation that avoids needlessly alarming consumers and undermining the significance of notification of a security breach by requiring notification only when the security and confidentiality of personal information is truly at risk. If the primary purpose of security breach legislation is to alert consumers to the possibility that their sensitive personal information may be subject to identity theft, it makes good sense to require companies to inform consumers only when there is a significant likelihood of identity theft. If there is little chance of identity theft or substantial harm, why needlessly alarm consumers when personal information is not at risk.

Enforcement and Rulemaking

It is also very important that there be uniform enforcement of notification standards. For this reason, ACLI strongly supports enforcement of insurers' compliance with security breach legislation exclusively by the Department of the Treasury. The Treasury Department has extensive experience with the insurance industry in connection with the implementation and enforcement of laws such as the

USA PATRIOT Act, the Terrorism Risk Insurance Act and the Bank Secrecy Act, as well as regulations promulgated by the Office of Foreign Asset Controls. As a result of this experience, ACLI believes that the Treasury is well positioned to implement and enforce the insurance industry's compliance with security breach notification legislation.

In the event it is not possible to provide for enforcement jurisdiction by the Treasury Department, ACLI recommends adoption of the enforcement structure set out in the GLB Act. Under this approach, an insurer's compliance with Federal breach of security notification legislation would be enforced exclusively by the insurance authority of the insurer's State of domicile. If this approach is used, ACLI also requests that the legislation State that it is the intent of the Congress that State insurance authorities enforce the legislation in a uniform manner.

If Federal security breach notification legislation provides for promulgation of implementing regulations, ACLI believes that the legislation should provide for the promulgation of uniform standards jointly by the relevant Federal agencies. Such an approach ensures that guidance will be applied uniformly across all industries and that the special needs of each sector of the economy will be taken into account and carefully considered. Adoption of joint standards has the added benefit of avoiding potential confusion among consumers because it provides certainty as to what consumers can expect to receive from companies that possess their sensitive information.

Conclusion

The issues you have before you today are indeed complex. They should be carefully studied and considered, as you are doing. ACLI anticipates that legislation you adopt will provide meaningful protection to consumers who might otherwise become victims of identity theft.

Thank you for your attention.

PREPARED STATEMENT OF OLIVER I. IRELAND

PARTNER, MORRISON & FOERSTER LLP

ON BEHALF OF THE

AMERICAN BANKERS ASSOCIATION

SEPTEMBER 22, 2005

Mr. Chairman and Members of the Committee, my name is Oliver Ireland. I am a Partner in the law firm of Morrison & Foerster LLP, practicing in the firm's Washington, DC office. I am here today on behalf of the American Bankers Association (ABA) to address the role of banking institutions in protecting consumers from identity theft and account fraud.

ABA, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership—which includes community, regional, and money center banks and holding companies, as well as savings associations, trust companies, and savings banks—makes ABA the largest banking trade association in the country.

In general terms, identity theft occurs when a criminal uses personal identifying information relating to another person (generally, a name, address, and Social Secu-

rity 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 consumer accounts can be used to initiate unauthorized charges to those accounts.

The issue of identity theft and account fraud, and related concerns about data security, are of paramount importance to banking institutions and the customers that we serve. Identity theft and account fraud can harm consumers and banking institutions, and challenge law enforcement. A major priority of the banking industry is stopping identity theft and account fraud before it occurs, and resolving those unfortunate cases that do occur. Both consumers and banking institutions benefit from a financial system that protects sensitive information relating to consumers, while remaining efficient, reliable, and convenient.

In my statement, I would like to emphasize three key points:

Banking Institutions Are Already Regulated

Unlike many other industries that maintain or process consumer information, banking institutions and their customer information security programs are subject to regulatory requirements and regular examinations. Banking institutions have a vested interest in protecting sensitive information relating to their customers, and work aggressively to do so.

Uniform Approach Will Promote Information Security

The security of sensitive consumer information will be promoted most effectively by a uniform national standard.

Security Breach Notification Requirements Should be Risk-Based

Any requirements should focus on situations that create a substantial risk of identity theft. Over-notification of consumers about breaches of information security will desensitize consumers and may lead consumers to ignore the very notices that explain the action they need to take to protect themselves from identity theft.

Banking Institutions Are Already Regulated

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

Banking institutions have a strong interest in protecting customer information. Banking institutions that fail to earn and to maintain the trust of their customers will lose those customers. In the competitive market for financial services, consumers tend to hold their banking institution accountable for any problems that they experience with their accounts or information, regardless of the actual source of the problem. For example, if fraud is committed on a bank account as a result of a breach of security at a data processor working for a retailer—an entity that the bank does not control—the customer is likely to first seek a solution through his or her bank. Therefore, information security is critical in order for banking institutions to maintain customer relations.

Because banking institutions do not impose the losses for fraudulent accounts on consumers and because banking institutions do not impose the losses associated with fraudulent transactions made on existing accounts on their customers, banking institutions incur significant costs from identity theft and account fraud. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs, including reputational harm. In addition, when a breach of information security occurs at a banking institution, the banking institution typically incurs other costs in responding to that breach. Accordingly, banking institutions aggressively protect sensitive information relating to their customers.

Existing Security Guidance

Earlier this year, the Federal banking agencies revised their guidance, originally issued in 2001 under Section 501(b) of the GLB Act, concerning the security of customer information. The revised guidance requires banking institutions to notify their customers of breaches of the security of sensitive information relating to those customers. We support the agencies' action and recommend their general approach as a model for going forward.

Already in force, the guidance requires banking institutions to establish and maintain comprehensive information security programs to identify and assess the

risks to customer information and then to address these potential risks by adopting appropriate security measures. The guidance requires that each banking institution's program for information security must be risk-based. Each banking institution must tailor its information security program to the specific characteristics of its business, customer information, and customer information systems, and must continuously assess the threats to its customer information and customer information systems. As those threats change, a banking institution must appropriately adjust or upgrade its security measures to respond to those threats.

A banking institution must consider access controls on its customer information systems, background checks for employees with responsibilities for access to customer information systems, and a response program in the event of unauthorized access to customer information. Not only do these requirements apply to customer information while in the banking institution's customer information systems, but the guidance also requires that a banking institution's contracts with its service providers must require those service providers to implement appropriate measures to protect against unauthorized access to or use of customer information.

A banking institution also must implement a risk-based response program to address instances of unauthorized access to customer information. A risk-based response program must include plans to:

- Assess the nature and scope of an incident of unauthorized access to customer information, and identify what customer information systems and the types of customer information that have been accessed or misused;
- Notify the banking institution's primary Federal regulator "as soon as possible" about any threats "to sensitive customer information;"
- Consistent with Suspicious Activity Report (SAR) regulations, notify appropriate law enforcement authorities and file SAR's in situations involving Federal criminal violations requiring immediate attention; and
- Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information. This could include, for example, monitoring, freezing, or closing accounts, while preserving records and other evidence.

Existing Notification Requirements

A critical component of the guidance is customer notification. The guidance dictates that when a banking institution becomes aware of a breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or will be misused. If the banking institution determines that misuse of the information "has occurred or is reasonably possible," it must notify, as soon as possible, those customers to whom the information relates. Customer notification may be delayed if law enforcement determines that notification will interfere with an investigation and provides a written request for a delay. The banking institution need only notify customers affected by the breach where it is able to identify those affected. If it cannot identify those affected, it should notify all customers in the group if it determines that misuse of the information is reasonably possible.

The customer notification standards established by the guidance combine tough security measures with practical steps designed to help consumers. These standards assure a timely, coordinated response that enables consumers to take steps to protect themselves, in addition to knowing the steps that their banking institution has taken to address the incident. The guidance permits banking institutions to focus their resources in a result-orientated way, without requiring unnecessary and possibly misleading customer notifications.

The customer notices required under these standards must be clear and conspicuous. The notices must describe the incident in general and the type of customer information affected. In addition, the notices must generally describe the banking institution's actions to protect the information from further unauthorized access and include a telephone number by which the customers can contact the institution concerning the incident. The notices should remind customers to remain vigilant over the following 12 to 24 months and to promptly report incidents of suspected identity theft to the institution. Where appropriate, the notices also should include:

- Recommendations that the customer review account statements immediately and report any suspicious activity;
- A description of fraud alerts available under the Fair Credit Reporting Act (FCRA), and how to place them;
- Recommendations that the customer periodically obtain credit reports and have incorrect information removed from those reports;
- Explanations of how to obtain a free credit report; and
- Further information about the agencies' guidance.

Risk-Based Standard

The agencies' approach encourages banking institutions to work on an ongoing basis with their regulators and customers, while requiring the institutions to take concrete and well-defined steps to address a suspected security breach. Immediately 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 deal with the problem. This 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. Customer data is stored and transmitted 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 itself in the wrong hands, it is often not in a readable or useable form. Banking institutions and their regulators need to retain the ability to react to each situation using a risk-based approach, which takes into account the ability to use the information to harm consumers through identity theft or account fraud.

Uniform Approach Will Promote Information Security

In order to provide meaningful and consistent protection for all consumers, all entities that handle sensitive consumer information—not just banking 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. These entities, including data brokers, such as ChoicePoint, universities, hospitals, private businesses, and even the Federal Deposit Insurance Corporation, have been the victims of security breaches. The information security breaches that have occurred at banking institutions over the past year represent only a small percentage of the breaches that have been reported. However, 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 can take steps to protect themselves.

It is not necessary to design a completely new system to address this issue. The regulations that already apply to banking institutions offer policymakers both a model and a measure of experience to aid in establishing umbrella consumer protections that span all industries that maintain sensitive consumer information. In considering the extension of bank-like regulation to unregulated industries that maintain sensitive consumer information, we believe that Congress should focus on a uniform approach that is designed to protect consumers from actual harm.

Uniformity Benefits Consumers

National uniformity is critical to preserving a fully functioning and efficient national marketplace. A score of state legislatures have already passed new data security or privacy bills that will take effect in 2006. While these 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. In some cases, a single State that adopts a unique requirement or omits a key provision can effectively nullify the policies of the other States.

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 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 be tailored to those circumstances and, within these circumstances, to the type of threat presented.

For example, a breach involving consumers' names and SSN's may expose them to the risk of identity theft, while a breach involving account information may pose no risk or cost to the consumer or may require the consumer to follow established procedures to reverse erroneous changes to their accounts. In each case, the need

for notification and the form of notification will differ. Any Federal legislative requirement must recognize and accommodate these differences.

Other Issues

While we believe that Federal legislation should focus on the security of sensitive consumer information and notification where a breach of that security threatens substantial harm to consumers, we recognize that in connection with this debate other issues, including the ability of consumers to place "security freezes" on their credit reports and the regulation of the display or sale of SSN's, have been raised. 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 to the potential for identity theft on particular accounts. It would be premature to discard this system 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 lift security freezes.

With respect to potential limitations on the display or sale of SSN's, it is important to avoid unintended consequences. For example, disrupting the many transactions that rely on these numbers, including the identification of bank customers for purposes of Section 326 of the USA PATRIOT Act, could harm consumers and national interests.

Finally, it is important to remember that regulatory compliance costs fall disproportionately on community banks. Any legislative solution to data security must consider these and other costs that would be imposed on community banks and their customers.

Conclusion

Bank institutions are proud of their record in protecting sensitive information relating to their customers, and will continue to work with the Committee and banking regulators to ensure consumers receive the highest level of protection possible.

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

RESPONSE TO WRITTEN QUESTIONS OF SENATOR BUNNING FROM IRA D. HAMMERMAN

Q.1. Do you have an opinion on what kind of notice should be sent out?

A.1. A notification requirement should be flexible, allowing financial institutions to deliver the notice in any manner designed to ensure that a customer can be reasonably expected to receive it, such as via website, regular mail, e-mail, or even oral notification depending upon the circumstances. In addition, firms need to have flexibility in the content of the notice so that the communications may be geared to the business and the particular situation.

Q.2. What do you consider harm? If account numbers are compromised, is that considered harm? If a Social Security number is compromised?

A.2. Before a financial institution is required to notify customers of a security breach of sensitive information, the firm must make a determination, after reasonable investigation, that there is a significant risk of identity theft or fraud. Notification for every incident, without regard to the risk of identity theft or fraud, would only overwhelm customers with notices, and only serve to needlessly frighten and confuse people.

A brokerage account number by itself—without other information—would likely have little value. A financial institution would need to assess the facts and circumstances of the entire incident to determine the risk to the customer. Monitoring account activity and/or merely changing an account number might limit the risk so that there is no need to notify the customer. Changing account numbers should not be deemed to cause substantial inconvenience.

SIA believes that the scope of the type of information that underpins any notification obligation should be carefully defined so that the obligation to notify only arises when the sensitive personal information acquired in the breach can likely be used to perpetrate the crime of identity theft or fraud upon a consumer. For instance, in the absence of a key, encrypted information is useless to others who acquire it and should be excluded from the definition of sensitive personal information. Consumers would benefit more from a specific definition of covered personal information which includes combinations of identifying data, as opposed to a broad definition that includes any single piece of information which could not alone be used to steal a consumer's identity.

Q.3. If the Committee put forward a data breach bill, what would you suggest be covered?

A.3. All businesses, not just financial institutions, should be required to protect the information that consumers provide to them, and provide notification of a data breach where there is significant risk of identity theft or fraud. Given that securities firms and other financial institutions are already covered by the Gramm-Leach-Bliley Act (GLB), any legislation addressing data breach should provide that the functional regulators of financial institutions subject to GLB have the exclusive authority to develop and enforce appropriate regulations. Moreover, legislation that extends beyond data

breach, possibly into unrelated areas of privacy, would lessen the chances for a prompt and appropriate Congressional response.

Q.4. Do any of you believe Social Security numbers should be truncated? Do you think their use should be limited? What protections do you suggest for use of the Social Security number?

A.4. SIA believes that in light of the restrictions on financial institutions' use and transfer of Social Security numbers under GLB, further restrictions on financial institutions are unnecessary. The GLB and its implementing regulations treat a financial institution's consumer's Social Security number as protected "nonpublic personal information." Therefore, each financial institution customer has the right to block a financial institution from selling or, subject to exceptions, transferring his or her Social Security number to a nonaffiliated third party or the general public. In short, a financial institution customer is fully protected with respect to a financial institution's transfer of Social Security numbers, yet legitimate and important uses of these numbers remain permissible.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR BUNNING FROM GILBERT T. SCHWARTZ

Q.1. Do you have an opinion on what kind of notice should be sent out?

A.1. Notices should be sent to consumers only when the security and confidentiality of personal information is at risk and where the breach is likely to lead to substantial financial loss or material inconvenience to consumers. Companies should be permitted to send notices by mail, e-mail, or other means that ensures that notice will be received by affected consumers. If the security breach affects a significant number of consumers, we believe that companies should be permitted to provide notice via notice to media in the area in which the affected consumers are located and by posting an appropriate notice on the companies' websites.

Q.2. Why do you consider harm? If account numbers are compromised, is that considered harm? If a Social Security number is compromised?

A.2. If a security breach is unlikely to result in harm to consumers, there is no need for consumers to take any action to protect themselves. Consumers should not be needlessly alarmed nor should companies be needlessly subjected to the considerable expense associated with providing notifications to consumers when the security and confidentiality of personal information is not at risk or when the breach is not likely to lead to substantial financial loss or material inconvenience to consumers. Accordingly, the compromise of account numbers or Social Security numbers should be considered harm only if it is likely to lead to substantial financial loss or material inconvenience to consumers.

Q.3. If the Committee put forward a data breach bill, who would you suggest be covered?

A.3. Federal data security breach legislation should cover any entity that maintains sensitive personal information about individuals.

Q.4. Do any of you believe Social Security numbers should be truncated?

A.4. It is of utmost importance to the insurance industry that information companies obtain about applicants, policyholders, insureds, and beneficiaries be associated with the correct individuals. A person's Social Security number is a unique identifier and is one of the most reliable means of assuring that the information insurers receive relates to the correct person. We are concerned that truncation of Social Security numbers could jeopardize insurers' ability to ensure that accurate and reliable information is obtained about the correct individual.

Q.5. Do you think their use should be limited?

A.5. It is critically important that insurers continue to have access to Social Security numbers to ensure the accuracy of information received about applicants, insureds, and policyholders and beneficiaries and to perform insurance business functions. In view of the significant role Social Security numbers play in processing and managing information needed by insurers in their normal operations, we believe that it is important to preserve the ability of insurers to serve existing and prospective customers. Accordingly, we believe that no limitations should be placed on the ability of insurers to use Social Security numbers.

Q.6. What protections do you suggest for use of the Social Security number?

A.6. We believe that Social Security numbers should be subject to administrative, technical, and physical safeguards to protect the confidentiality and integrity of Social Security numbers in the possession of any business entity.

RESPONSE TO WRITTEN QUESTIONS OF SENATOR BUNNING FROM OLIVER I. IRELAND

Q.1. Do you have an opinion on what kind of notice should be sent out?

A.1. As stated in our written testimony, the ABA believes that notice of a security breach should only be required where consumers need to act to protect themselves from substantial harm resulting from the breach. More specifically, notice should only be required where it is reasonably likely that information involved in a security breach will be misused in a manner causing substantial harm, such as identity theft or account fraud, to the consumers. The type of notice that should be provided should depend on the type of sensitive information involved in the breach and the risks surrounding misuse of that information.

Consumers face different risks depending on what type of sensitive information is involved in a security breach. For example, if a breach involves only a consumer's name and address in combination with the consumer's Social Security number (SSN) or taxpayer identification number (collectively, sensitive personal information), the consumer may face a risk of identity theft because the thief may be able to use that information to open fraudulent accounts in the consumer's name. However, the consumer would not face a risk of account fraud because this information is not sufficient to access specific accounts. Conversely, if a breach involves only a consumer's name and financial account number in combination with any password or code that is required to access the account (sen-

sitive account information), the consumer would not face a risk of identity theft because this information alone cannot be used to open fraudulent accounts. However, the fraudster may be able to use that information to commit account fraud on existing accounts.

The appropriate response by consumers to a security breach also depends on the type of sensitive information involved in the breach and the risks surrounding the misuse of that information. For example, if a breach involves sensitive personal information, a consumer can take several steps to prevent or mitigate the effects of identity theft resulting from the breach. The consumer can place an initial fraud alert on his or her credit file at a consumer reporting agency (CRA) in order to alert creditors that an identity thief may attempt to open a fraudulent account in the consumer's name and also to trigger creditors' duties to verify an applicant's identity and confirm that the application is not the result of identity theft. The consumer also may wish to monitor his or her credit report to determine whether any fraudulent accounts have been opened in his or her name. However, the consumer would not need to monitor or close his or her existing financial accounts because there is not a risk of account fraud.

If a security breach involves sensitive account information, a consumer will not be at a risk of identity theft and should not expend time and valuable resources to address a risk that does not exist. Sensitive account information generally will not enable an identity thief to open fraudulent accounts. Instead, the consumer should monitor the account to which the information relates, and promptly report any fraudulent transactions made on that account. Federal law, including the Truth in Lending Act and the Electronic Fund Transfer Act, and State law, in the form of the Uniform Commercial Code, provide strong remedies for consumers to address account fraud. In most instances when a consumer reports a fraudulent transaction to a banking institution, the institution will promptly credit the consumer's account for the transaction, often requiring only a phone call by the consumer.

Because consumers face different risks when a security breach involves different types of sensitive information, and because the appropriate response to these risks differs, consumers should receive different notices that take into account these different risks and responses. For example, if a security breach involves sensitive personal information, the notice to consumers should include: (1) a brief description of the breach, including the type of sensitive personal information involved in the breach; (2) the Federal Trade Commission contact information to obtain model forms and procedures for consumers who may be at risk of identity theft; and (3) the nationwide CRAs' contact information for obtaining credit reports and filing fraud alerts. If a security breach involves sensitive account information, the notice to consumers should include: (1) a brief description of the breach, including the type of sensitive account information involved in the breach; and (2) a recommendation that they review account statements and report suspicious activity or transactions to the account-holding institution.

Q.2. Why do you consider harm? If account numbers are compromised, is that considered harm? If a Social Security number is compromised?

A.2. It is appropriate to focus security breach notification requirements on those breaches in which consumers face a risk of substantial harm from identity theft or account fraud. If notice is not limited to those breaches involving a risk of substantial harm, consumers will be inundated with notices, and likely will disregard all security breach notices, including in circumstances where they actually need to take steps to protect themselves from identity theft or account fraud. In addition, the costs of providing notice will increase dramatically.

Whether or not consumers are at risk of substantial harm from identity theft or account fraud as a result of a security breach will depend on the facts surrounding that breach. In many instances, consumers in fact should not be at risk of substantial harm from identity theft or account fraud even though a security breach may have involved sensitive personal information or sensitive account information. For example, if a breach involves sensitive personal information or sensitive account information that was encrypted or redacted (or is otherwise unuseable), consumers should not be at risk of substantial harm from identity theft or account fraud because the information cannot be used in that form to commit identity theft or account fraud. Similarly, if a breach involves sensitive account information, such as credit card numbers, but the account-holding institution maintains a sophisticated neural network or fraud detection program to detect and block fraudulent transactions before they occur, consumers are not at risk of substantial harm from account fraud. For example, credit card issuers often proactively telephone consumers about suspected account fraud and provide new accounts if the consumers confirm that fraud has occurred. The fraudulent transactions never even appear on a statement. In these cases, the only "harm" suffered by a consumer may be answering a brief phone call.

Q.3. If the Committee put forward a data breach bill, who would you suggest be covered?

A.3. In order to provide meaningful and consistent protection for all consumers, all entities that hold sensitive personal information or sensitive account information should be subject to similar data security and security breach notification requirements with respect to that information. As we noted in our testimony, Title V of the Gramm-Leach-Bliley Act (GLBA), and associated rulemakings and guidance, require banking institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized access or use and to notify customers when there is a breach of security with respect to sensitive information relating to those customers. However, most businesses, including retailers and CRA's, are not subject to data security and/or security breach notification requirements.

Q.4. Do any of you believe Social Security numbers should be truncated?

A.4. In certain instances, requiring the truncation of SSN's, or otherwise limiting the use of SSN's, may be appropriate. For example, under the Fair Credit Reporting Act, a consumer who requests a file disclosure from a CRA also may request that the CRA truncate the consumer's SSN in that disclosure. However, in everyday trans-

actions, banking institutions and other businesses use SSN's as an identifier for important and legitimate purposes, including compliance with Federal law. Any decision by Congress to limit the use of SSN's or to impose restrictions with respect to the use of SSN's, such as truncation or encryption requirements, must include exceptions that permit the important and legitimate uses of SSN's by banking institutions and other businesses, including for the prevention of fraud, the facilitation of credit checks, the identification of prospective employees, and compliance with Federal law.

The use of the SSN as an identifier in everyday transactions has grown dramatically over the years. Generations ago, when consumers lived, worked and shopped locally, their good name in the community enabled them to obtain credit, employment, insurance, and other services. With today's more transient population and with the advent of national markets due to the Internet and other improvements in communication, the vast majority of businesses obtain and use SSN's to identify consumers. Today, critical decisions about credit, employment, insurance, and other services depend on the availability of SSN's.

SSN's provide a unique number that is issued by the Federal Government and can be used to link information to a consumer. More than 280 million people live in the United States, and tens of thousands of these people share the same name. And, many people who share the same name also share other identifying information, such as the city and State of residence or month and year of birth. Unlike other identifying information, such as name, address and marital status, an individual's SSN does not change over that individual's life, and no other living person shares that number.

Banking institutions and other businesses, including insurance companies, utility companies, and cell phone providers, use SSN's to obtain credit reports and credit scores and to obtain public record information about individuals. The nationwide CRA's maintain credit files on nearly 200 million individuals. These files are linked to SSN's. If businesses cannot obtain SSN's and provide these numbers to CRA's when requesting credit reports and credit scores, it would be difficult if not impossible to ensure that the credit report or credit score they receive relates to the appropriate consumer. This process of identifying and approving consumers would be slower and far less accurate without SSN's. Any delays in approving credit would be particularly hard on retail stores that offer "instant credit" to their customers. Similarly, public records serve as an important source of information about individuals. SSN's are necessary to ensure that public record information is matched to the appropriate individuals.

If banking institutions cannot obtain and use SSN's to verify the identity of consumers, fraud, including identity theft, could increase substantially. Banking institutions use identification services based on SSN's to properly identify consumers and to prevent identity theft and other fraud. In addition, if SSN's cannot be obtained, banking institutions will not be able to comply with Federal laws designed to prevent money laundering and terrorist financing. For example, the regulations implementing Section 326 of the USA PATRIOT Act require every bank, as part of its customer identification program, to collect taxpayer identification numbers, typi-

cally SSN's, and to verify the identities of individuals seeking to open new accounts.

The ability of businesses to screen applicants for employment also would be impaired by limiting the use or availability of SSN's. Many businesses obtain SSN's from job applicants in order to obtain credit reports or to conduct background checks. For example, businesses ranging from banking institutions to nursing homes, day care facilities, and security companies obtain and use SSN's in order to determine job applicants' histories, including whether they have criminal records. And, for tax purposes, all employers are required to obtain and enter on every W–2 form each employee's name and SSN.

Although it may be possible to develop a secure and dependable replacement for SSN's, any such system would require years, if not decades, to implement, could substantially increase personal verification and transactions costs and, ultimately, likely would be just as susceptible to fraud as SSN's. In the meantime, any decision to limit the use or availability of SSN's must include exceptions that permit the important and legitimate uses of SSN's by banking institutions and other businesses, including for the prevention of fraud, the facilitation of credit checks, the identification of prospective employees, and compliance with Federal law.

Although arguably the "truncation" of SSN's could have a lesser impact than an outright limitation on the use or disclosure of SSN's, any truncation of SSN's would impair the current legitimate business uses of SSN's. For example, only allowing use of the last four digits of an SSN could result in a significant number of errors in identifying individuals.

Q.5. Do you think their use should be limited?

A.5. See response to question 4.

Q.6. What protections do you suggest for use of the Social Security number?

A.6. Any entity or person that maintains or possesses an SSN relating to a consumer should be required to protect the security and confidentiality of that number and also to notify the consumer if the security of that number is breached and the consumer is at risk of substantial harm from identity theft.