

**SOCIAL SECURITY NUMBERS IN
COMMERCE: RECONCILING
BENEFICIAL USES WITH THREATS
TO PRIVACY**

HEARING
BEFORE THE
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS
SECOND SESSION

MAY 11, 2006

Serial No. 109-91

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

29-388PDF

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 ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan

Ranking Member

HENRY A. WAXMAN, California

EDWARD J. MARKEY, Massachusetts

RICK BOUCHER, Virginia

EDOLPHUS TOWNS, New York

FRANK PALLONE, JR., New Jersey

SHERROD BROWN, Ohio

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

ELIOT L. ENGEL, New York

ALBERT R. WYNN, Maryland

GENE GREEN, Texas

TED STRICKLAND, Ohio

DIANA DEGETTE, Colorado

LOIS CAPPS, California

MIKE DOYLE, Pennsylvania

TOM ALLEN, Maine

JIM DAVIS, Florida

JAN SCHAKOWSKY, Illinois

HILDA L. SOLIS, California

CHARLES A. GONZALEZ, Texas

JAY INSLEE, Washington

TAMMY BALDWIN, Wisconsin

MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*

DAVID CAVICKE, *General Counsel*

REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

JAN SCHAKOWSKY, Illinois

Ranking Member

MIKE ROSS, Arkansas

EDWARD J. MARKEY, Massachusetts

EDOLPHUS TOWNS, New York

SHERROD BROWN, Ohio

BOBBY L. RUSH, Illinois

GENE GREEN, Texas

TED STRICKLAND, Ohio

DIANA DEGETTE, Colorado

JIM DAVIS, Florida

CHARLES A. GONZALEZ, Texas

TAMMY BALDWIN, Wisconsin

JOHN D. DINGELL, Michigan

(EX OFFICIO)

CONTENTS

	Page
Testimony of:	
Leibowitz, Hon. Jon, Commissioner, Federal Trade Commission.....	16
Ireland, Oliver I., Partner, Morrison & Foerster, LLP, on behalf of Financial Services Coordinating Council	30
McDonald, Susan, President, Pension Benefit Information	39
Steinfeld, Lauren, Former Associate Chief Counselor, Office of Management and Budget	44
Lively, Jr., H. Randy, President and CEO, American Financial Services Association	49
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center	53

**SOCIAL SECURITY NUMBERS IN
COMMERCE: RECONCILING
BENEFICIAL USES WITH THREATS TO
PRIVACY**

THURSDAY, MAY 11, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,

Washington, DC.

The subcommittee met, pursuant to notice, at 2:45 p.m., in Room 2123, Rayburn House Office Building, Hon Cliff Stearns [chairman] presiding.

Present: Representatives Stearns, Deal, Bass, Blackburn, Barton (Ex Officio), Schakowsky, Markey, and DeGette.

Staff Present: David Cavicke, General Counsel; Shannon Jacquot, Counsel; Chris Leahy, Policy Coordinator; Will Carty, Professional Staff Member; Billy Harvard, Legislative Clerk; Consuela Washington, Minority Senior Counsel; and Alec Gerlach, Minority Staff Assistant.

MR. STEARNS. Good afternoon, everybody. The subcommittee will come to order. I am pleased that we are holding this important hearing on the use of Social Security numbers and the implication use of personal privacy. I would like to thank Chairman Barton for bringing this issue to the fore. Our work on data security did not address Social Security numbers, because we believe it is a complex issue that needs more focus and distinct treatment from securing personal information, notice, and yes, privacy issues that arise in the commercial world--a world is fueled by information, incredible technology that facilitates our tremendous progress, and one that is starting to present us with some very serious and complex challenges that require our attention today.

If you are an American citizen, you, without exception, have one of those long string of numbers associated with our individual identity called a Social Security number. As Chairman Barton has pointed out, in 1935, the Social Security Administration was directed to create an accounting system that would be able to track how much we put into the Social Security pot in taxes so we can get credit for those contributions when we act to withdraw them. The Social Security Administration was

not directed to create a unique personal identifier for commercial purposes.

The issues that are before us today have arisen because government and private businesses quickly realized how good the idea was, a unique identifier, and soon adopted it for their own use, whether for tax administration, fraud prevention, or to send out marketing information. I think all of those uses can be legitimate as long as they are conducted with the utmost respect for the personal privacy of the individual, including adhering to the security principles outlined in our data security bill. A bill designed to prevent misuse and fraud. My colleagues, I do, however, want to learn more about those cases when a customer is denied goods or services because he or she decides they don't want to furnish their Social Security number.

I think most Members here don't want to give it out. We understand the emotional issues involved when confronted by such a request, and we are continuing to be confronted. So I would like to ask today's witnesses to help us understand why that is something business needs to have these days, and is it an anti-fraud mechanism or what?

I would also like to suggest our witnesses take us through the concept addressed in perhaps three of the major bills that have been introduced in this Congress and deal with the issue of Social Security number use and personal privacy, particularly the bill H.R. 1745, the Social Security Number Privacy and Identity Prevention Act of 2005, introduced by my colleague from Florida, Mr. Shaw. Chairman Shaw has done great work in this area, and I commend him for his work as a tireless advocate for protecting the privacy of consumers and maintaining the integrity of Social Security numbers, balancing the benefits that accrue to consumers from private use Social Security numbers with the harm caused by identity theft is a difficult feat.

In addition, because identity theft is a very important consumer protection issue, we would like to hear specifics about that issue and how it relates to Social Security number misuse and security from the Federal Trade Commission. The FTC data indicates that in a 1 year period of time from September 2002 to September 2003, over 10 million people were victims of identity theft. This is a big cost to consumers and businesses both in terms of money lost and time spent trying to clear up names and credit reports. The Federal Trade Commission has done a tremendous job in gathering important statistical information regarding identity theft. This will help us in policy decisions we make in this committee.

I look forward to a general update from the FTC on the state of identity theft today and would like to hear what ideas the commission has for reducing the occurrence of identity theft. So I would like to thank

everybody for joining us today, especially Commissioner Leibowitz, who had to juggle some scheduling to be here, and I look forward to his testimony, as we take a dive into this very interesting and important issue.

And with that, I will conclude and ask Ms. DeGette, who is standing in for the Ranking Member, for her opening statement.

[The prepared statement of Hon. Cliff Stearns follows:]

PREPARED STATEMENT OF THE HON. CLIFF STEARNS, CHAIRMAN, SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

I am very happy that we are holding this important hearing on the use of social security numbers and the implications for personal privacy. I'd like to thank Chairman Barton for bringing this issue to the fore. Our work on data security did not address social security numbers because we believe it is a complex issue that needs more focus and distinct treatment from securing personal information, notice, and yes, privacy issues that arise in the commercial world – a world that is fueled by information, incredible technology that facilitates our tremendous progress, and one that is starting to present us with very serious and complex challenges that require attention now.

If you have a heartbeat and are an American citizen, you will, almost without exception, have one of those long strings of numbers associated with our very person, called the social security number. As Chairman Barton has pointed out, back in 1935, The Social Security Administration was directed to create an accounting system that would be able to track how much we put into the social security pot in taxes so we can get credit for those contributions when we act to draw on them. The Social Security Administration was not directed to create a unique personal identifier for commercial purposes. The issues that are before us today have arisen because government and private business quickly realized how good the idea was – a unique identifier – and soon adopted it for their own use – whether for tax administration, fraud prevention, or to send marketing. I think all those uses can be legitimate as long as they conducted with the utmost respect for the personal privacy, including adhering to the security principles outlined in our data security bill- a bill designed to prevent misuse and fraud. I do, however, want to learn more about those instances when a consumer is denied goods or services because he or she decides they don't want to furnish their social security number. I don't like to give it out so I understand the emotional issues involved when confronted by such a request. I'd like to ask today's witnesses to help us understand why that is something business need to do these days – is it an anti-fraud mechanism or what?

I also would like to suggest that our witnesses take us through the concepts addressed in the major bills that have been introduced this Congress and deal with the issues of social security number use and personal privacy, particularly the bill HR 1745, the Social Security Number Privacy and Identity Theft Prevention Act of 2005, introduced by my good friend and colleague from Florida, Mr. Shaw. Chairman Shaw has done a tremendous amount of work in this area. I commend him for his work as a tireless advocate for protecting the privacy of consumers and maintaining the integrity of social security numbers. Balancing the benefits that accrue to consumers from private use of social security numbers with the harm caused by identity theft is a difficult feat.

In addition, because identity theft is a very important consumer protection issue, we would like to hear specifics about that issue and how it relates to social security number misuse and security from the Federal Trade Commission. FTC data indicates that in a one-year period of time, from September 2002 to September 2003, over 10 million people were victims of identity theft. This is a significant cost to consumers and

businesses both in terms of money lost and time spent trying to clear up names and credit reports. The Federal Trade Commission has done a tremendous job in gathering important statistical information regarding identity theft. This will help us in policy decisions we make. I look forward to a general update from the Federal Trade Commission on the state of identity theft today and would like to hear what ideas the Commission has for reducing the occurrence of identity theft.

Again, I thank everyone for joining us today, especially Commissioner Liebowitz, who had to juggle some scheduling and logistical issues to be here today. Thank you. We look forward to the testimony. This is a very important hearing as my Subcommittee begins to take a deep dive into the issue surrounding personal privacy in the commercial world.

MS. DEGETTE. Thank you, Mr. Chairman, and Ms. Schakowsky should be along shortly. She has an amendment up on the floor right now. So she will--

MR. STEARNS. I understand.

MS. DEGETTE. --be along. First of all, I want to welcome Commissioner Liebowitz, who I just found out is a fellow graduate of the New York University School of Law.

MR. LEIBOWITZ. You might have had better grades than me, though.

MS. DEGETTE. Hmm?

MR. LEIBOWITZ. You might have had better grades than me, though.

MS. DEGETTE. I don't know. We will talk about that later. I also want to thank you, Mr. Chairman, for having this series on privacy. I know it has long been an issue that you have chaired personally and really, really made it an effort to have full, full hearings. I think that the wide range of views among different industries and consumer groups, coupled with the complexity of the issue, has made it a challenging task to craft legislation, and so I am impressed by the bills that really go in depth on this issue, and I look forward to debating their merits.

The first privacy hearing that we had in this series was actually 5 years ago, in 2001, and at that hearing, I talked about how many of my constituents have been contacting me and express an interest in and concern about personal privacy. This, of course, remains even more so true today, and I would say their concerns have grown more accurate.

Just this morning we saw, for example, that the NSA is apparently trying to collect records of every single telephone call made--these are not international terrorist phone calls but made domestically in this country. And one has to ask oneself, what is the nexus between people making domestic phone calls and the NSA collecting all of the information on the phone numbers that are making and receiving the phone calls, how could that possibly have a nexus to national security and fighting terrorism?

And I talked just a few minutes ago to Chairman Barton, and I talked to Mr. Markey earlier, and we all share a concern about government

agencies and others collecting more and more data about people with seemingly no controls over this.

And so I am hoping Chairman Barton will hold some hearings on this issue, which is within the preview of this committee because it is of real concern. And a similar issue I hear about from constituents all the time is the growing requirement that a Social Security number be given to conduct business with various companies, whether it is getting a credit card, opening an account, or whatever else. And people always ask me, is it legal for companies to require a Social Security number to do business with them? Do they have any recourse if they are refused a transaction or if they are turned away for applying for something when they do not provide their Social Security number? So clearly, there is a great deal of discomfort among many about giving out their Social Security number, even for a seemingly legitimate purpose.

And I will tell you, the more recent revelations like the ones that we see today with the NSA taking the phone numbers of legitimate domestic phone calls is only going to make people feel more and more uncomfortable about giving out any personal information, and they are really going to begin wondering if big brother is looking over them, and I am sure, Mr. Chairman, you and the other members of this committee are hearing from our constituents. The drum beat is growing ever louder, and we have got to do something to secure people's privacy and their private information.

Social Security numbers, interestingly, are seen as the gold standard of identifying information, and yet, the more that groups use them, then the more the Social Security numbers are out there, then the greater likelihood it is that these Social Security numbers will be given out and stolen and used for fraud.

So with respect to this hearing on the one hand, we have the current practice of businesses who are trying to protect themselves from fraud, requiring Social Security numbers, and then on the other hand, we have consumers who are increasingly reluctant to give their Social Security numbers out, and for increasingly good reasons.

So how do we reconcile this? I think it is going to be an interesting balancing act, but I have got to tell you, I feel like the tipping point has been reached, and we have got to make a real effort not just at the Social Security numbers, but at all of people's identifying information and communications. How do we protect people's security, while at the same time encouraging commerce and encouraging legitimate national security uses. And with that, Mr. Chairman, I will yield back the balance of my time.

MR. STEARNS. I thank the gentlelady. Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I want to thank you for your attention on the issue, and Mr. Leibowitz, I want to thank you for taking the time to be with us today and for being here to present the information and to join us as we look at the use of Social Security numbers with financial transactions and also with commerce.

Congress has enacted several laws to guard against the misuse of consumer information, but it absolutely has not been enough. In the past few years, identity theft has become the fastest growing crime in America and has cost consumers and businesses in the neighborhood of \$50 billion. We were astounded at the number of people that showed up at an identity theft town hall in our district, and we were appalled and really quite concerned with some of the stories that they had to tell.

One of the major glaring examples is the occurrence of security breaches at several data brokers. These breaches have subjected many consumers to theft of personal information, and I appreciate this committee has passed the Data Act to address that problem, and now we know that we must look at the role of Social Security numbers in the era of e-commerce. I know that companies do want a quick and reliable method of identifying people to conduct business, yet we do have to balance the privacy concerns that exist, and as we move forward and look at data security and privacy, we understand that the world of e-commerce presents many new opportunities for individuals. At the same time we have to recognize that it does present many challenges that new technologies are presenting wonderful opportunities, but at the same time, there are challenges and there are concerns and there is truly a need for us to review our existing policies. And, Mr. Chairman, I thank you for your leadership and your willingness to review those existing policies. I look forward to the information we will have in this hearing, and looking at how we can achieve balance, and I yield back.

MR. STEARNS. Thank you. The gentleman from Massachusetts is recognized.

MR. MARKEY. Thank you, Mr. Chairman. And thank you for having this hearing. This hearing, at my request, of the full committee Chairman and yourself, Mr. Chairman, is meant to consider my proposed legislation H.R. 1078, the Social Security Number Protection Act, as well as other legislative ideas on how to protect Americans from the misuse of their Social Security numbers. H.R. 1078 would bring a halt to unregulated commerce in Social Security numbers. It does not establish an absolute prohibition on all commercial use of the number, but it would make it a crime for a person to sell or purchase Social Security numbers in violation of the rules promulgated by the Federal Trade Commission. The FTC would be given the power to restrict the sale of

Social Security numbers, determine appropriate exemptions, and to enforce civil compliance and the bill's restrictions.

We thank Mr. Leibowitz for being here, and the other experts that are here to talk to us today, and what could be a more appropriate day, given the fact that Mr. Rotenberg has a lawsuit against the NSA to determine exactly how the NSA is spying on Americans, than on a day that we learn that there has been a new telecom merger between NSA and AT&T. And it is the last takeover in this chain of mergers which has occurred. NSA, AT&T now stands for now spying on Americans, anytime you talk, NSA, AT&T, the new America, the new telecom NSA America.

So we have got a new slogan for the NSA and AT&T, "Reach out and tap someone." And what we see is an incredible violation of the privacy of Americans by the Federal government. The argument is made that they are going to compile every phone call ever made in the United States, I think that we have now reached a point of privacy crisis in the name of security. The price being paid is the privacy of all Americans, and it is too high a price to pay.

Here in the Social Security area, from Amy Boyer through thousands of other examples, we see what happens when people's privacy, their Social Security number is used as an identifier. What the NSA and AT&T have made clear today is that this is just part of a larger puzzle, where technology makes possible things which were unimaginable when we were younger, and it is our responsibility to make sure that we safeguard, we secure that private information so that the DNA of each family isn't just a commodity out there for purchase by the highest bidder, notwithstanding the consequences for the history of that family. I thank you, Mr. Chairman, for having this hearing.

MR. STEARNS. I thank the gentleman. The Chairman of the full committee, Mr. Barton from Texas.

CHAIRMAN BARTON. Thank you, Mr. Chairman. I apologize for being delayed. We were doing a hearing on gasoline prices in the same committee hearing room, and it went longer than expected. I made a commitment to Congressman Markey at a full committee markup on the data security bill, that we would address the issue of Social Security number privacy. And I want to thank you, Chairman Stearns, for honoring my commitment to hold this hearing so I could honor the commitment I made to Congressman Markey at that markup.

I share Mr. Markey's concerns about the widespread abuse, and I want to highlight abuse, of Social Security numbers. I believe, like Congressman Markey, that not enough is being done to protect this unique personal identifier. The Data Act which passed this committee, I think, 42-0, recently would go a long way towards ensuring proper

security for databases that contain Social Security numbers and other personal information. I am proud of our committee's work on that bill, and am working very hard, as late as noon today, to get that bill to the floor of the House.

While the Data Act is a very important component of protecting Social Security numbers and sensitive personal data, the bill does not address the issue surrounding the use of Social Security numbers. There are a number of complex issues in this area.

The nature of business has evolved over the past several decades to serve a population that engages much more frequently in interstate commerce. The rise of the Internet has popularized electronic commerce. Also rising unfortunately is the risk of criminal activity, and for crooks, a Social Security number is like a key to the bank.

Twenty years ago, nobody thought much about showing their number. Their Social Security number on a driver's license or, I apologize, a store clerk writing it on checks. Now we know that this number is an integral part of our identity, and there are lots and lots of people who want to steal our identity. Our economic system allows us to conduct transactions anywhere, anytime almost instantaneously.

In this world of e-commerce, companies have to know who they are dealing with. That is why they believe consumer's Social Security numbers is a necessary component to many transactions, because it has evolved to become a unique and required identifier for almost every significant aspect of our lives. Its value is even more important than simply a claim on a future government retirement check, which was its original intention, because it is so important.

My belief, and Congressman Markey's belief, is Congress needs to act to put in place new protections. I recognize that removing the link between our Social Security number and our personal accounts is difficult, and maybe it will turn out to be impractical. What I want to see is a development of an alternative identifier and then we can judge the suitability of removing Social Security numbers all together. Sometimes using Social Security numbers as a commercial identifier speeds business, and that is a benefit, no question about it, both to the companies and to the consumers. That said, there are also many situations in which there's no apparent reason or consumer benefit to provide a Social Security number.

This committee has looked at many issues in this area and will continue to consider other issues in this area. We continue to wonder, for example, whether businesses can or should require consumers to provide a Social Security number in order to buy a product or service.

I recently purchased a new cell phone for my charitable foundation for my personal use in making charitable calls. I had to give my Social

Security number three times in the process of being approved for that cell phone, and my Social Security number was not necessary to prove that I had the financial ability to pay for the phone or really, that I was who I said I was since I also had to give my driver's license number. But if I didn't give my Social Security number, I wasn't going to get that phone. I just don't see that that is a necessity.

Further, once a business has a consumer's Social Security number, can they share it? Can they sell it? And if so, to who? Having your number is one thing. Selling it, I think, or using it for a purpose without your permission is quite another. And how should a company go about getting a person's consent to transfer a Social Security number to another entity?

These were important questions to which there are not always simple answers. But one question to which there is an easy answer is whether our Social Security number should be sold by Internet data brokers to anyone willing to pay. Indistinguishable from sales of sports scores or stock quotes that to me is a no-brainer. There is no legitimate reason why my Social Security number should be sold or used by a business without a relationship with me, and without my knowledge and consent, period, end of debate.

There are some uses of Social Security numbers that many people agree provide benefits beyond the potential for harm. Locating criminals, locating witnesses, enforcing child support obligations, and other purposes are clearly legitimate. It gets more difficult when we are talking about locating people, generally confirming identity outside of fraud prevention, and marketing just generic products and services. The potential for harm, which has been well documented by this committee, raises serious questions about using Social Security numbers for those purposes.

I expect this committee will consider legislation on Social Security numbers this year. I want to repeat that. I expect this committee will consider legislation on Social Security numbers this year.

I hope the Ways and Means Committee will also act on an important bill by Congressman Clay Shaw, one of their subcommittee chairmen. And I support his effort to get that bill out of the Ways and Means Committee. But I intend to use the jurisdiction of the Energy and Commerce Committee to move a Social Security bill out of this committee this year.

We have a very distinguished group of witnesses here today to work through some of these issues. I want to thank all of you for participation and, in particular, I want to thank Commissioner Leibowitz who has been with us before. I understand that you have made some significant changes to your schedule to be here, and I appreciate it. I look forward

to the testimony today, Mr. Chairman. I yield back the 3 minutes and 35 seconds that I have already overextended.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY
AND COMMERCE

Thank you, Mr. Chairman, for holding this hearing today. I made a commitment to Congressman Markey at the Full Committee markup on data security to address the issue of Social Security number privacy. I share Mr. Markey's concerns about widespread abuse of Social Security numbers and believe, like him, that not enough is being done to protect this unique personal identifier. The DATA Act, recently reported out of this Committee, goes a long way toward ensuring proper security for databases that contain Social Security numbers and other personal information. I am proud of this Committee's work on that bill and will continue my efforts to see that bill move to the House floor.

While the DATA Act is a very important component of protecting social security numbers and sensitive personal data, the bill does not address the issues surrounding the *use* of Social Security numbers. There are a number of complex issues to consider in this area. The nature of business has evolved over the past several decades to serve a population that engages much more frequently in interstate commerce. The rise of the Internet has popularized electronic commerce. Also rising is the risk of criminal activity, and for crooks, a Social Security number is the key to the bank. Twenty years ago, nobody thought much about showing the Social Security number on a driver's license or about a store clerk writing it on our checks. Now we know that number is an integral part of our identity, and lots of people want to steal our identity.

Our economic system allows us to conduct transactions anywhere and anytime, and almost instantaneously. In this world of e-commerce, companies have to know who they're dealing with. That's why they believe a consumer's Social Security number is a necessary component to many transactions. Because it has evolved to become a unique and required identifier for almost every significant aspect of our lives, its value is even more important than simply a claim on a future government retirement check. Because it is so important, Congress may need to act to put in place new protections.

I recognize that removing the link between our Social Security number and our personal accounts is difficult, and maybe it will turn out to be impractical, too. What I want is the development of an alternative, and then we can judge the suitability of removing Social Security numbers altogether.

Sometimes, using Social Security numbers as commercial identifiers speeds business, and that's a benefit to companies, to consumers, and to the economy. That said, there are also many situations in which there is no apparent reason or consumer benefit to providing a Social Security number. This Committee has looked at many issues in this area, and will continue to consider others. We continue to wonder, for example, whether businesses can or should require consumers to provide a Social Security number in order to buy a product or service? If so, which businesses? Further, once a business has a consumer's Social Security number, can they share it? Can they even sell it, and to whom? Having your number is one thing. Selling it, I think, is another. And how should a company go about getting a person's consent to transfer a Social Security number to another entity?

These are important questions to which there are not always simple answers. But one question to which there **IS** an easy answer is whether our Social Security numbers should be sold by Internet data brokers to anyone willing to pay, indistinguishable from sales of sports scores or stock quotes. That's a no-brainer. There is no legitimate reason

why my number should be sold or used by a business without a relationship with me, and without my knowledge and consent.

There are some uses of Social Security numbers that many people would agree provide benefits far beyond the potential for harm. Locating criminals, locating witnesses, enforcing child support obligations, and other noble purposes are clearly legitimate. It gets more difficult when we are talking about locating people generally, confirming identity (outside of the fraud prevention context), and marketing products and services. The potential for harm, which has been well documented by this Committee, raises serious questions about using social security numbers for these services.

I expect this Committee will consider legislation on Social Security numbers later this year. I hope the Ways and Means Committee will also act on an important bill by Congressman Clay Shaw and send us the part that is in this committee's jurisdiction.

We have a very distinguished group of witnesses here today to work through some of these issues with us. I want to thank you all for your participation. In particular, I want to thank Commissioner Leibowitz. I understand you made some significant changes to your schedule to be here and we do appreciate it. I look forward to the testimony today and yield back the balance of my time.

MR. STEARNS. And I thank the Chairman for his leadership. The Ranking Member, Ms. Schakowsky is recognized.

MS. SCHAKOWSKY. Thank you, Chairman Stearns. I apologize for being late. I had an amendment to address. I also want to thank Mr. Markey for his great leadership on this issue, and I am very encouraged by Chairman Barton's remarks.

First, let me say that the topic of protecting consumers' privacy could not be timelier. Before I get into the subject of our hearing, I want to say a few, not as clever as Mr. Markey, things today about the latest instance of big business jumping into bed with big brother. That was my effort. As the USA Today article on NSA: "NSA has a massive database of Americans' phone calls. Telecoms help government collect billions of domestic records," reveals AT&T, BellSouth and Verizon have been providing the records of millions of Americans to the National Security Agency without consumers' knowledge or consent.

We have entered a time where consumers' rights and privacy are for sale, and it turns out the Government may be the best customer. In our fight to protect consumers from unsavory characters, like ID thieves, we also need to fight the erosion of our civil liberties of what our government is doing. With that said, I do believe today's hearing is important because protecting Social Security numbers is vital in the fight for consumers' privacy in the fight against identity theft.

I think it is important that our subcommittee delve into how the Social Security number is used and explore legislative solutions to curb the overuse and abuse of it. Unfortunately, Chairman Stearns, our States, Florida and Illinois, have ranked in the top 10 for number of victims of identity theft each year for the last 3 years. A recent report by the Government Accountability Office refers to the Social Security number

as “The identifier of choice for public and private entities.” It went on to say that the Social Security number is the most sought-after information by identity thieves.

Many in the financial, housing, and insurance and other industries claim they need consumers’ Social Security numbers to protect their business and supposedly consumers from risk. However, the reality is that requiring Social Security numbers for everything from opening a bank account to signing a cell phone contract, as Chairman Barton experienced, shifts all the risk to the consumer and all the advantages to ID thieves.

Having a consumer Social Security number is like having the master key to his or her life. It can throw open the door to detailed financial information, unlock your private medical information, and in at least one tragic instance, provided the stalker of Amy Boyer with where she would be and at what time. He used that information to end her life.

While most of us give our Social Security numbers to whatever business asks for it without question, or at least many of us do, we should be asking a lot of questions. Why does a landlord need the master key to my life to rent me an apartment? Does my doctor really need to store my health care records under my Social Security number? What does an insurance company use my Social Security number for? And why is it that with more and more transactions, I am being required to give my Social Security number and put my finances, personal safety, and medical privacy in jeopardy?

We are all so used to being asked for our numbers, we may not give enough thought to what that other party does with the Social Security number. That company may sell them. The numbers may be sent over the Internet for legitimate purposes but may not be protected in those transmissions. Our new accounts often stay linked to our Social Security numbers. The numbers may be displayed on forms or files that are not adequately protected. And as the GAO points out, even government agencies aren’t keeping them as safe and secure as they should.

This should give everyone pause. If we can limit how other parties use our numbers, then we can establish a good framework to prevent the misuse of the key to our personal financial information. We know that identity theft is financially and emotionally devastating. Anyway, that is why I am glad that we are considering what we can do to protect consumers.

I am proud to support Mr. Markey’s bill, H.R. 1078, the Social Security Number Protection Act, which would restrict the display and sale of Social Security numbers, and I hope today’s hearing is just the beginning of our discussions but will lead to a concrete proposal and passage of a bill in the end.

I thank you for this hearing and look forward to hearing from our witnesses.

MR. STEARNS. I thank the gentlelady.

The gentleman from New Hampshire.

MR. BASS. Thank you very much, Mr. Chairman. This is a very relevant and important hearing. Amy Boyer was my constituent. She was murdered in 1999. The stalker and murderer bought her Social Security number over the Internet and other information about her.

The other day I went to a well-known retailer to purchase a clothes dryer, and in order to get a \$50 rebate, I had to give the retailer my Social Security number. I don't know whether that was really relevant, but I had to. My daughter, at the age of 6 or 7 years old, signed up for travel soccer, and she could not participate in travel soccer without giving her Social Security number.

The Social Security number was created, as has been said by the Chairman, back in the 1930s for purposes of identifying people who qualified for a defined benefit retirement program. Clearly, the use of these numbers is totally out of control at this point. I am heartened by Chairman Barton's commitment to move a bill in this Congress that will move decisively to protect the holders of Social Security numbers who have that Social Security number not because it is a privilege, like a driver's license or any other kind of document, but that it is a requirement that every American have, and that this number is then used for all sorts of different purposes that are not generic to its original issuance.

So I welcome the Commissioner of the Federal Trade Commission here today and the other witnesses that will be appearing, and I thank you for having this hearing.

MR. STEARNS. I thank the gentleman.

The gentleman from Georgia, Mr. Deal.

MR. DEAL. I waive.

MR. STEARNS. The gentleman waives his opening statement.

With that, we move to the first panel and we recognize the Federal Trade Commission, the Honorable Jon Leibowitz, Commissioner. And if you will just pull the mike close to you, turn it on, we welcome you with your opening statement.

**STATEMENT OF HON. JON LEIBOWITZ, COMMISSIONER,
FEDERAL TRADE COMMISSION**

MR. LEIBOWITZ. Chairman Stearns, Ranking Member Schakowsky, Ms. DeGette, Mr. Bass, Mr. Deal, it is always a pleasure to come back to this committee, whether in the context of helping to prohibit telephone

pretexting, stop spam or spyware, or determine the best ways to address the uses and, obviously, the misuses, of Social Security numbers.

Today I will be talking about that aspect of privacy, the balance between the benefits of Social Security numbers and the harms that misuse can cause. That is really at the heart of the debate, and I commend you for holding this hearing.

With your permission, I ask that my full written statement be submitted for the record. My oral remarks, though, are my own comments, and do not necessarily reflect the views of the Commission or any other individual commissioner.

MR. STEARNS. So ordered.

MR. LEIBOWITZ. Thank you. At the FTC, we take our obligation to protect privacy very, very seriously. We have brought more than a dozen cases involving data security as well as six spyware and adware cases--we have several more in the pipeline--almost 20 financial and cell phone pretexting cases, and more than 80 spam cases.

Just yesterday, we announced a complaint, together with a settlement, against a major real estate services firm, Nations Title, that failed to safeguard information properly and disposed of that information cavalierly. Among other things, we allege that the company threw out detailed customer files, which included Social Security numbers, in a dumpster just outside of its corporate headquarters. Just think about that for a minute.

As you know, Social Security numbers do serve many important functions. For example, the credit reporting system hinges on the availability of Social Security numbers to match consumers accurately with their financial information. Other uses of Social Security numbers include locating lost beneficiaries and collecting child support. Indeed, SSNs are often used to prevent fraud. But Social Security numbers are a substantial contributor to the worst form of identity theft: Having new accounts opened in your name.

Not surprisingly, Americans today are very concerned about protecting their identities. And rightly so. I think as you mentioned, Mr. Chairman, about 10 million people each year are victims of identity theft, and more than 3 million people each year have new accounts opened fraudulently in their names.

If your identity is stolen, you may struggle for months or years to clear your name, and the emotional impact can be severe. American businesses pay a heavy price as well, as someone mentioned, I think it was Mrs. Blackburn, \$50 billion a year in costs.

The key, then, is to find the right balance between permitting the beneficial uses of Social Security numbers while keeping them out of the hands of criminals and other people who shouldn't have them. There is

no panacea, of course, but it helps to approach the problem in a multifaceted way.

Users of Social Security numbers should migrate, I think, towards using less sensitive identifiers whenever possible. For example, some colleges still use SSNs on ID cards, though doing so is clearly unnecessary. And Chairman Barton mentioned his experience when he was getting a cell phone. My wife had exactly the same experience just a few weeks ago at Tyson's Corner, where she was asked to say in public what her Social Security number was, and it was very troubling to her. And I don't want to say that the Social Security number wasn't necessary in that circumstance, but companies overall do need to do a better job of securing consumer data. They have a fundamental legal responsibility to do so.

The Commission, of course, can sue firms that misrepresent their security procedures or fail to take reasonable steps to secure or dispose of sensitive information. Two of our most recent cases, as you know, Mr. Chairman, ChoicePoint and Card Systems, involved massive data breaches that led to numerous instances of identity theft. In each, the Commission alleged that the company failed to take reasonable measures to protect consumer information, including, in ChoicePoint, Social Security numbers. These actions, along with Nations Title, are just the most recent in a long line of cases that send a message to businesses: protect consumers' personal information.

And you can further strengthen our hand and help ensure that Social Security numbers are better protected from fraud by enacting strong data security legislation that requires all businesses to safeguard sensitive personal information, gives notice to consumers if there is a breach--whether under your reasonable risk standard or the significant risk standard that we suggested last year--and allows us to fine companies that don't live up to their legal obligations.

Consumer and business education are also critical. We receive between 15,000 and 20,000 contacts each week from people seeking advice on avoiding identity theft or coping with its consequences. We provide information and assistance to simplify the recovery process. The Commission also works with the business community to try to promote a culture of security.

Yesterday, I was in our calling center when a man phoned in. He was very anxious because his Social Security number had just been discovered on a suspect arrested by the police. He was worried that his identity had been stolen. And our staff did a terrific job with him, gave him the appropriate advice, including putting a fraud alert on his credit report.

Also yesterday, we launched a major new campaign designed to give advice to anyone who wants to learn about identity theft, and it is entitled “Deter, Detect, and Defend.” It is a tool kit that provides specific suggestions so consumers can prevent identity theft before it happens and reduce the damage after it occurs. It is available in both English and Spanish. It is very, very good, and we have a handful of packets here for Members and staff and we will bring them up to the dais.

Finally, the Commission assists criminal law enforcement through our operation of the Identity Theft Clearinghouse, a nationwide database that includes more than a million identity theft complaints. Law enforcers ranging from the FBI to the Postal Service to local sheriffs use the clearinghouse to aid in their investigations.

Mr. Chairman, determining how best to keep Social Security numbers out of the hands of wrongdoers, without giving up the benefits that their use provides, is a daunting challenge, and there is no simple solution. Still, by working together, there is much that we can do. This committee, as always on privacy matters, will be crucial to striking the appropriate balance.

Thank you so much. I am happy to answer any questions.
[The prepared statement of Hon. Jon Leibowitz follows:]

PREPARED STATEMENT OF THE HON. JON LEIBOWITZ, COMMISSIONER, FEDERAL TRADE COMMISSION

I. INTRODUCTION

Mr. Chairman, Ms. Schakowsky, and members of the Subcommittee, I am Jon Leibowitz, Commissioner of the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s views on identity theft and Social Security numbers (“SSNs”).

The Commission has a broad mandate to protect consumers generally and to combat identity theft specifically. Controlling identity theft is an issue of critical concern to all consumers – and to the Commission. The FTC serves a key role as the central repository for identity theft complaints, facilitates criminal law enforcement in detecting and prosecuting identity thieves, and provides extensive victim assistance and consumer education. In recognition of the need to protect sensitive consumer information and prevent identity theft, the FTC recently created a new Division of Privacy and Identity Protection. This division – which consists of staff with expertise in privacy, data security, and identity theft – addresses cutting-edge consumer privacy matters through aggressive enforcement, as well as rulemaking, policy development, and outreach to consumers and businesses.

This testimony describes the ways in which SSNs are collected and used, their relationship to identity theft, current laws that restrict the use or transfer of consumers’ personal information, and the Commission’s efforts to help consumers avoid identity theft or remediate its consequences.

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

II. THE IDENTITY THEFT PROBLEM

Identity theft is a pernicious crime that harms both consumers and businesses. Recent surveys estimate that nearly 10 million consumers are victimized by some form of identity theft each year.² The costs of this crime are staggering. The Commission's 2003 survey estimated that identity theft cost businesses approximately \$50 billion, and cost consumers an additional \$5 billion in out-of-pocket expenses, over the twelve-month period prior to the survey.³ The 2003 survey looked at two major categories of identity theft: (1) misuse of existing accounts; and (2) the creation of new accounts in the victim's name. The 2003 survey found that the costs imposed by new account fraud were substantially higher than the misuse of existing accounts.⁴

III. USES AND SOURCES OF SOCIAL SECURITY NUMBERS

SSNs today play a vital role in our economy. With 300 million American consumers, many of whom share the same name,⁵ the unique 9-digit SSN is a key identification tool for businesses, government, and others.⁶ For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file and that they are providing a credit report on the correct consumer.⁷ Businesses and other entities use these reports to evaluate the risk of providing to individuals services, such as credit, insurance, home rentals, or employment. Timely access to consumer credit, as well as the overall accuracy of credit reporting files, could be compromised if SSNs could not be used to match consumers to their financial information. Additionally, SSNs are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. SSN databases also are used to fight identity fraud – for example, to confirm that an SSN provided by a loan applicant does not, in fact, belong to someone who is deceased.⁸ Without the ability to use SSNs as a personal identifier and fraud prevention tool, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

SSNs are available from both public and private sources. Public records in city and county government offices across the country, including birth and death records, property records, tax lien records, voter registrations, licensing records, and court records, often contain consumers' SSNs.⁹ Increasingly, these records are being placed online where

² See Federal Trade Commission - Identity Theft Survey Report (2003), <http://www.ftc.gov/os/2003/09/synovaterreport.pdf> and Rubina Johannes, 2006 Identity Fraud Survey Report (2006), <http://www.javelinstrategy.com/research>. A free summary of the 2006 Identity Fraud Survey Report is available at <http://www.bbb.org/alerts/article.asp?ID=651>.

³ Federal Trade Commission - Identity Theft Survey Report at 6 (2003), <http://www.ftc.gov/os/2003/09/synovaterreport.pdf>.

⁴ Id.

⁵ According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

⁶ See General Accounting Office, Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information (GAO 04-01) (2004).

⁷ See Federal Trade Commission - Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003 at 38-40 (2004), <http://www.ftc.gov/reports/facta/041209factarpt.pdf>.

⁸ The federal government also uses the SSN as an identifier, for example, as both an individual's Medicare and taxpayer identification number. It also is used to administer the federal jury system, federal welfare and workmen's compensation programs, and military draft registration. See Social Security Administration, Report to Congress on Options for Enhancing the Social Security Card (Sept. 1997), www.ssa.gov/history/reports/ssnreportc2.html.

⁹ Local and state governments are reducing their reliance on SSNs for many administrative purposes in response to identity theft concerns. For example, only a few states still use SSNs as drivers license numbers. See David A. Lieb, Millions of Motorists Have Social Security Numbers

they can be accessed easily and anonymously.¹⁰ There also are a number of private sources of SSNs, including consumer reporting agencies that include name, address, and SSN as part of the “credit header” information on consumer reports. Data brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties.¹¹

The misuse of SSNs, however, can facilitate identity theft. For example, new account fraud - the most serious form of identity theft - is often possible only if the thief obtains the victim’s SSN. The challenge is to find the proper balance between the need to keep SSNs out of the hands of identity thieves, while giving businesses and government entities sufficient means to attribute information to the correct person. Restrictions on disclosure of SSNs also could have a broad impact on such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts. Moreover, as referenced above, regulation or restriction of the availability of SSNs in public records poses substantial policy and practical concerns.

IV. CURRENT LAWS RESTRICTING THE USE OR DISCLOSURE OF SOCIAL SECURITY NUMBERS

There are a variety of specific statutes and regulations that restrict disclosure of certain consumer information, including SSNs, in certain contexts. In addition, under some circumstances, entities are required to have procedures in place to ensure the security and integrity of sensitive consumer information such as SSNs. Three statutes that protect SSNs from improper access fall within the Commission’s jurisdiction: Title V of the Gramm-Leach-Bliley Act (“GLBA”);¹² Section 5 of the Federal Trade Commission Act (“FTC Act”);¹³ and the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”),¹⁴ amending the Fair Credit Reporting Act (“FCRA”).¹⁵

A. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (“GLBA”) imposes privacy and security obligations on “financial institutions.”¹⁶ Financial institutions are defined broadly as those entities

on Licenses, The Boston Globe, Feb. 6, 2006, http://www.boston.com/news/local/massachusetts/articles/2006/02/06/millions_of_motorists_have_social_security_numbers_on_licenses/. In some cases, however, governments still use SSNs as identifiers when it is not essential to do so. See Mark Segraves, Registering to Vote May Lead to Identity Theft, WTOP Radio, Mar. 22, 2006, <http://www.wtop.com/?nid=428&sid=733727>.

¹⁰ Improved access to public records has important public policy benefits, but at the same time raises privacy concerns. Some public records offices redact sensitive information such as SSNs, but doing so can be very costly. The Commission has recognized the sensitive nature of SSNs, even when they are contained in publicly available records. For example, in response to a comment on the DSW order, the Commission stated that “[C]ertain publicly available records, such as court records, contain Social Security numbers and other highly sensitive information that can be used to perpetrate identity theft.” The Commission response letter is available at http://www.ftc.gov/os/caselist/0523096/0523096DSW_LettertoCommenterBankofAmerica.pdf.

¹¹ Some data brokers have announced that they are voluntarily restricting the sale of SSNs and other sensitive information to those with a demonstrable and legitimate need. See Social Security Numbers Are for Sale Online, Newsmax.com, Apr. 5, 2005, <http://www.newsmax.com/archives/articles/2005/4/4/155759.shtml>.

¹² 15 U.S.C. §§ 6801-09.

¹³ 15 U.S.C. § 45(a).

¹⁴ Pub. L. No. 108-159, 117 Stat. 1952.

¹⁵ 15 U.S.C. §§ 1681-1681x, as amended.

¹⁶ 15 U.S.C. § 6809(3)(A).

engaged in “financial activities” such as banking, lending, insurance, loan brokering, and credit reporting.¹⁷

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of the GLBA¹⁸ from disclosing nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.¹⁹ However, the GLBA includes a number of statutory exceptions under which disclosure is permitted without having to provide notice and an opt-out. These exceptions include consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.²⁰ Entities that receive information under an exception to the GLBA are subject to the reuse and redisclosure restrictions of the GLBA Privacy Rule, even if those entities are not themselves financial institutions.²¹ In particular, the recipients may only use and disclose the information “in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received].”²²

Entities can obtain SSNs from consumer reporting agencies, generally from the credit header data on the credit report. However, because credit header data is typically derived from information originally provided by financial institutions, entities that receive this information generally are limited by the GLBA’s reuse and redisclosure provision.

2. Required Safeguards for Customer Information

The GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers, whether directly or from other financial institutions.²³ The FTC’s Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,²⁴ requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires a plan that accounts for each entity’s particular circumstances – its size and complexity, the nature

¹⁷ 12 C.F.R. §§ 225.28, 225.86.

¹⁸ See 15 U.S.C. § 6802; Privacy of Consumer Financial Information, 16 C.F.R. Part 313 (“GLBA Privacy Rule”).

¹⁹ See 15 U.S.C. § 6809. The GLBA defines “nonpublic personal information” as any information that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, SSN, address, telephone number, mother’s maiden name, and prior addresses. See, e.g., 65 Fed. Reg. 33,646, 33,680 (May 24, 2000) (the FTC’s Privacy Rule).

²⁰ 15 U.S.C. § 6802(e).

²¹ 16 C.F.R. § 313.11(a).

²² *Id.*

²³ 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (“Safeguards Rule”).

²⁴ The Federal Deposit Insurance Corporation, the National Credit Union Administration (“NCUA”), the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, and state insurance authorities have promulgated comparable information safeguards rules, as required by Section 501(b) of the GLBA. 15 U.S.C. § 6801(b); see, e.g., Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616-41 (Feb. 1, 2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps (for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers) in implementing their plans.²⁵

B. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”²⁶ Under the FTC Act, the Commission has broad jurisdiction over a wide variety of entities and individuals operating in commerce. Prohibited practices include making deceptive claims about one’s privacy procedures, including claims about the security provided for consumer information.²⁷

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.²⁸ The Commission has used this authority to challenge a variety of injurious practices, including companies’ failure to provide reasonable and appropriate security for sensitive customer data.²⁹ The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

C. The Fair and Accurate Credit Transactions Act of 2003

The FACT Act amended the FCRA to include a number of provisions designed to increase the protection of sensitive consumer information, including SSNs. One such provision required the banking regulatory agencies, the NCUA, and the Commission to promulgate a coordinated rule designed to prevent unauthorized access to consumer report information by requiring all users of such information to have reasonable procedures to dispose of it properly and safely.³⁰ This Disposal Rule, which took effect on June 1, 2005, should help minimize the risk of improper disclosure of SSNs.

In addition, the FACT Act requires consumer reporting agencies to truncate the SSN on consumer reports at the consumer’s request when providing the reports to the consumer.³¹ Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

²⁵ The Commission previously has recommended that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC’s existing GLBA Safeguards Rule to companies that are not financial institutions. See Statement of Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 7, <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>.

²⁶ 15 U.S.C. § 45(a).

²⁷ Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984).

²⁸ 15 U.S.C. § 45(n).

²⁹ Other practices include, for example, allegations of unauthorized charges in connection with “phishing,” high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, SSNs, passwords, or other sensitive information. See *FTC v. Hill*, No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), <http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm>; *FTC v. C.J.*, No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), <http://www.ftc.gov/os/2003/07/phishingcomp.pdf>.

³⁰ 16 C.F.R. Part 382 (“Disposal of Consumer Report Information and Record Rule”).

³¹ 15 U.S.C. § 1681g(a)(1)(A). The FTC advises consumers of this right through its consumer outreach initiatives. See, e.g., the FTC’s identity theft prevention and victim recovery guide, *Take Charge: Fighting Back Against Identity Theft* at 5 (2005), available at <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.pdf>.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain other specific classes of information, including SSNs. For example, the Driver's Privacy Protection Act ("DPPA")³² prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance. The Health Information Portability and Accountability Act ("HIPAA") and its implementing privacy rule prohibit the disclosure to third parties of a consumer's medical information without prior consent, subject to a number of exceptions (such as, for the disclosure of patient records between entities for purposes of routine treatment, insurance, or payment).³³ Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."³⁴

E. FTC Enforcement Actions

Over the past year or so, reports have proliferated about information compromises at U.S. businesses, universities, government agencies, and other organizations that collect and store sensitive consumer information, including SSNs. Some of these incidents reportedly have led to identity theft, confirming that security breaches can cause real and tangible harm to consumers, businesses, and other institutions.

Since 2001, the Commission has brought thirteen cases challenging businesses that have failed to take reasonable steps to protect sensitive consumer information in their files.³⁵ Two of the Commission's most recent law enforcement actions arose from high-profile data breaches that occurred last year. In the first case, the Commission alleged that a major data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the FCRA³⁶ and the FTC Act.³⁷ The Commission's complaint alleged that ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in a consumer protection case – and \$5 million in consumer redress for identity theft victims. The Order also requires ChoicePoint to implement a number of strong data security measures, including bi-annual audits to ensure that these security measures are in place.

In the second action, the Commission reached a settlement with CardSystems Solutions, Inc., the card processor allegedly responsible for last year's breach of credit and debit card information for Visa and MasterCard, which exposed tens of millions of consumers' credit and debit numbers.³⁸ This case addresses the largest known

³² 18 U.S.C. §§ 2721-25.

³³ 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

³⁴ 45 C.F.R. § 164.530(c).

³⁵ Documents related to these enforcement actions generally are available at <http://www.ftc.gov/privacy/index.html>.

³⁶ 15 U.S.C. §§ 1681-1681x, as amended. The FCRA specifies that consumer reporting agencies may only provide consumer reports for certain "permissible purposes." ChoicePoint allegedly approved as customers individuals whose applications had several indicia of fraud, including false credentials, the use of commercial mail drops as business addresses, and multiple applications faxed from the same public commercial location. The FTC's complaint alleged that ChoicePoint did not have a permissible purpose in providing consumer reports to such individuals and failed to have reasonable procedures to verify prospective subscribers.

³⁷ *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006).

³⁸ In the Matter of CardSystems Solutions, Inc., FTC File No. 052-3148 (proposed settlement posted for public comment, Feb. 23, 2006). The settlement requires CardSystems and its successor corporation to implement a comprehensive information security program and obtain audits by an

compromise of sensitive financial data to date. As in the ChoicePoint case, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. These settlements provide important protections for consumers and also provide important lessons for industry about the need to safeguard consumer information.

V. THE COMMISSION'S EFFORTS TO COMBAT IDENTITY THEFT

In addition to our efforts to ensure that businesses take reasonable steps to safeguard sensitive consumer information, the Commission works in many other ways to address the identity theft problem. Pursuant to the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act"),³⁹ the Commission has implemented a program that assists consumers, businesses, and other law enforcers.

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft, for consumers concerned about identity theft. Every week, the Commission receives about 15,000 to 20,000 contacts from victims and consumers seeking information on how to avoid identity theft. The callers to the hotline receive counseling from trained personnel who provide information on steps they can take both to prevent identity theft and to resolve problems resulting from the misuse of their identities. Victims are advised to: (1) obtain copies of their credit reports and have a fraud alert placed on them;⁴⁰ (2) contact each of the creditors or service providers with which the thief has established or accessed an account to request that the account be closed and to dispute any associated charges; and (3) report the theft to the police and, if possible, obtain a police report. The police report is useful in demonstrating to purported creditors and debt collectors that the consumer is a victim of identity theft, and serves as an "identity theft report" that can be used for exercising various victims' rights granted by the FACT Act.⁴¹ The Commission's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaints into the Clearinghouse.

The Commission also has taken the lead in developing and disseminating identity theft-related consumer education materials, including an identity theft primer, ID Theft: What It's All About, and a victim recovery guide, Take Charge: Fighting Back Against Identity Theft. The Commission alone has distributed more than 2.1 million copies of the Take Charge booklet (formerly known as ID Theft: When Bad Things Happen To Your Good Name) since its release in February 2000 and has recorded more than 2.4 million visits to the Web version. The Commission also maintains the identity theft website,

independent third-party professional every other year for 20 years. As noted in the FTC's press release, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

³⁹ Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

⁴⁰ The FACT Act added a requirement that consumer reporting agencies, at the request of a consumer, place a fraud alert on the consumer's credit report. Consumers may obtain an initial alert if they have a good faith suspicion that they have been or are about to become an identity theft victim. The initial alert must stay on the file for at least 90 days. Actual victims who submit an identity theft report can obtain an extended alert, which remains in effect for up to seven years. Fraud alerts require users of consumer reports who are extending credit or related services to take certain steps to verify the consumer's identity. See 15 U.S.C. § 1681c-1.

⁴¹ These include the right to an extended fraud alert, the right to block fraudulent trade lines on credit reports and to prevent such trade lines from being furnished to a consumer reporting agency, and the ability to obtain copies of fraudulent applications and transaction reports. See 15 U.S.C. § 1681 et seq., as amended.

www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

Last fall, the Commission, together with partners from law enforcement, the technology industry, and nonprofits, launched OnGuard Online, an interactive, multi-media resource for information and up-to-the minute tools on how to recognize Internet fraud, avoid hackers and viruses, shop securely online, and deal with identity theft, spam, phishing, and file-sharing.⁴²

In addition, yesterday the Commission launched a major new consumer education campaign called Deter, Detect, and Defend – Fighting Back Against Identity Theft. The campaign provides specific information on what consumers can do to reduce their risk of falling victim to ID theft, keep a close eye on their personal information, and move quickly to minimize the damage if identity theft occurs. The centerpiece of the campaign is a turnkey toolkit, available in both English and Spanish, that gives consumers resources for teaching clear, actionable tips on how to avoid becoming a victim of identity theft, protect their sensitive financial information, and reduce the damage should they suspect ID theft. The Commission will join with partners in the public and private sectors, including other federal agencies, industry associations, and consumer and civic organizations to make this information available where it is needed – in neighborhoods, at the workplace and on campuses across the country.

The Commission also has developed ways to simplify the recovery process. One example is the ID Theft Affidavit, included in the Take Charge booklet and on the website. This standard form was developed in partnership with industry and consumer advocates for victims to use in resolving identity theft debts. To date, the Commission has distributed more than 293,000 print copies of the Affidavit and has recorded more than 1.1 million hits to the Web version.

B. Working with Industry

The private sector can play a key role in combating identity theft by reducing its incidence through better security and authentication. The Commission works with institutions to promote a “culture of security” by identifying ways to spot risks to the information they maintain and keep it safe.

Among other things, the Commission has disseminated advice for businesses on reducing risks to their computer systems⁴³ and on compliance with the Safeguards Rule.⁴⁴ Our emphasis is on preventing breaches before they happen by encouraging businesses to make security part of their regular operations and corporate culture. The Commission also has published Information Compromise and the Risk of Identity Theft: Guidance for Your Business, a booklet on managing data compromises.⁴⁵ This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

In 2003, the Commission held a workshop that explored the challenges consumers and industry face in securing their computers. Titled “Technologies for Protecting Personal Information: The Consumer and Business Experiences,” the workshop also examined the role of technology in meeting these challenges.⁴⁶ Workshop participants,

⁴² See www.onguardonline.gov. OnGuard Online is also available in Spanish. See www.AlertaEnLinea.gov.

⁴³ Security Check: Reducing Risks to Your Computer Systems, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm>.

⁴⁴ Financial Institutions and Customer Data: Complying with the Safeguards Rule, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

⁴⁵ Information Compromise and the Risk of Identity Theft: Guidance for Your Business, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/idthrespond.pdf>.

⁴⁶ See workshop agenda and transcripts available at www.ftc.gov/bcp/workshops/technology. See Staff Report available at <http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf>.

including industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups, identified a range of challenges in safeguarding information and proposed possible solutions.

C. Working with Law Enforcement

A primary purpose of the Identity Theft Act was to provide law enforcement with access to a centralized repository of identity theft victim data to support their investigations. The Commission operates this database as a national clearinghouse for complaints received directly from consumers and through numerous state and federal agencies, including the Social Security Administration's Office of Inspector General.

With over 1.1 million complaints, the Clearinghouse provides a detailed snapshot of current identity theft trends as reported by the victims themselves. The Commission publishes data annually showing the prevalence of complaints broken out by state and city.⁴⁷ Since its inception, over 1,400 law enforcement agencies have registered for access to the Clearinghouse database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week. The Clearinghouse also gives access to training resources, and enables users to coordinate their investigations.

The Commission also encourages use of the Clearinghouse through training seminars offered to law enforcement. In cooperation with the Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, and the American Association of Motor Vehicle Administrators, the Commission began organizing full-day identity theft training seminars for state and local law enforcement officers in 2002. To date, this group has held 20 seminars across the country. More than 2,880 officers have attended these seminars, representing over 1,000 different agencies. This week three new seminars are being held in California.

To further assist law enforcers, the Commission staff developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse, and refers the reports to financial crimes task forces and others for further investigation and possible prosecution. In addition, analysts from the FBI, U.S. Secret Service, and Postal Inspection Service work on-site at the FTC, developing leads and supporting ongoing investigations for their agencies.

VI. CONCLUSION

The crime of identity theft is a scourge, causing enormous damage to businesses and consumers. The unauthorized use of consumers' SSNs is an important tool of identity thieves, especially those seeking to create new accounts in the victim's name. Although current laws place some restrictions on the use or disclosure of SSNs by certain entities under certain circumstances, this information is still otherwise available from both public and private sources, thereby enabling identity thieves to obtain SSNs through legal means as well as illegal means.

At the same time, SSNs are an important driver of our market system. Businesses and others rely on SSNs to provide many important benefits for consumers and to fight identity theft.

⁴⁷ See Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Jan. 2006), available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>. The Commission also conducts national surveys to learn how identity theft impacts the general public. The FTC conducted the first survey in 2003 and is conducting a second survey this spring. See Federal Trade Commission - Identity Theft Survey Report (Sept. 2003), available at <http://www.ftc.gov/os/2003/09/synovaterreport.pdf>.

There are a number of things that government, industry, and consumers can do to help stem the tide of identity theft. First, both government and industry need to consider what information they collect and maintain from or about consumers and whether they need to do so. Entities that possess sensitive consumer information should continue to enhance their procedures to protect it. The Commission will continue its law enforcement and outreach efforts to encourage and, when necessary, require better protections.

Second, industry should continue the development of improved fraud prevention methods to stop identity thieves from misusing the consumer information they have managed to obtain. In this regard, the FACT Act should prove instrumental by requiring the bank regulatory agencies, the NCUA, and the FTC to develop jointly regulations and guidelines for financial institutions and creditors to identify possible risks of identity theft.⁴⁸

Third, the Commission will continue and strengthen its efforts to empower consumers by providing them with the knowledge and tools to protect themselves from identity fraud and to deal with the consequences when it does occur. As discussed above, new consumer rights granted by the FACT Act should help consumers minimize the damage.

Finally, the Commission will continue to assist criminal law enforcement in detecting and prosecuting identity thieves. The prospect of serious jail time hopefully will discourage those considering identity theft from perpetrating this crime.

The Commission looks forward to continuing to work with Congress to address ways to reduce identity theft.

MR. STEARNS. Thank you, Mr. Commissioner. I will start here with the questions. We have a vote, but I think we can make progress here with a couple.

Let's say that Congress decided in the bill to restrict the use of Social Security numbers in commerce so we wouldn't have the thing with Mr. Bass' daughter, or Chairman Barton getting a new cell phone, or your wife, or anything like that. What would be the cost? Would it be a lot of cost for industry to stop using that as an identifier?

And what else would be the identifier? Would it be something like a State-issued driver's license number? What could you predict in the future?

MR. LEIBOWITZ. If you immediately banned all Social Security number use in a commercial context tomorrow, some businesses would be able to switch, I think, from Social Security numbers to other identifiers. There might be some dislocation. The Social Security number is the most underprotected and overused identifier in America today, but if you banned them entirely, there would be a lot of dislocation and a lot of legitimate transactions that use a Social Security number to identify who someone is so that they can get, for example, a mortgage or credit, would be hard to do. It might not be hard with Jon Leibowitz, there aren't too many of us out there, but there are 23,000

⁴⁸ 15 U.S.C. § 1681m(e).

Michael Smiths in America. So making sure you have the right one can be challenging.

MR. STEARNS. What would the identifier be, if it wouldn't be the Social Security number?

MR. LEIBOWITZ. Well, I don't think we know that. If you banned the Social Security number, perhaps a variety of different identifiers would take their place. There might be one new identifier that would begin to dominate the market, and then you would have some of the same problems with the new identifier that you have today with Social Security numbers.

MR. STEARNS. So the President signs the bill today and it prohibits, let's say, starting tomorrow, business from refusing to do business with a consumer without receipt of a Social Security number. What would the consumer transaction look like then?

MR. LEIBOWITZ. Again, many consumer transactions are done without Social Security numbers, and some consumer transactions are done with Social Security numbers that don't need to be.

MR. STEARNS. I know in Florida we have these very sophisticated licenses with pictures and holograms and everything, and that is getting to be much used. The number on the license is being used.

MR. LEIBOWITZ. Well, that might become--

MR. STEARNS. The new identifier.

MR. LEIBOWITZ. The default identifier. It sounds like Florida has a fairly sophisticated identifier for its license. And what might happen, and I think the bills that you are considering in this committee, whether it is the Shaw bill or the Markey bill, have a series of exemptions--for law enforcement, for national security, for emergencies, or with the consent of consumers. And I know in the Markey bill, at least there is sort of a catch-all provision that would allow us to set up the regulations for appropriate commercial uses.

So if President Bush signed a bill, presumably it would have this committee's imprimatur and it would strike the appropriate balance.

MR. STEARNS. Let me, just for a moment, talk about Mr. Markey's bill, H.R. 1078. Does this bill give the FTC the authority to write a regulatory exception for fraud prevention purposes?

MR. LEIBOWITZ. Yes. I mean we would want to work with this committee, but the short answer is yes, it would. It is a good point of departure to start a debate in this committee for what that law should look like.

MR. STEARNS. In dealing with the Shaw bill, is there any aspect about it that you feel would be not workable; that should be changed at all?

MR. LEIBOWITZ. Well, Mr. Chairman, I am not as familiar with the Shaw bill, because that is in the Ways and Means Committee. I do know it is similar in many ways to Mr. Markey's bill. I believe it has a provision that would drop Social Security numbers below the line, and that may cause a fair amount of dislocation, because some people don't need an entire credit report. This might force or encourage more people to get such credit reports, which includes even more sensitive personal information.

And if you dropped it below the line, I believe, and made it part of the Fair Credit Reporting Act, you would need to think about appropriate exemptions because the FCRA doesn't have an exemption for law enforcement. And I think that would be very, very useful, certainly from our perspective as a civil law enforcement agency.

MR. STEARNS. This is my last question. If a private entity adds a Social Security number from a public record to a database, should that public information, that public record information necessarily be treated differently suddenly because you add a Social Security number to it than other nonpublic information in a database?

MR. LEIBOWITZ. If I understand your question, I think under current law, you should look to where the information came from. So if the information is a Social Security number and came from a public database, it should be continued to be treated as such. The information in the database, which may be under Gramm-Leach-Bliley's reuse and redisclosure provisions, or maybe under the FCRA, should be treated under that statute.

MR. STEARNS. My time has expired.

Ms. Schakowsky.

MS. SCHAKOWSKY. Thank you. I want to ask what legislative measures do you think would be effective in better securing, in general, consumers' financial information, I mean, considering data security legislation?

MR. LEIBOWITZ. Well, I think you put your finger on it. The data security legislation that came out of this committee unanimously would go a long way towards ensuring that all businesses maintain safeguards for sensitive consumer information, and it would give us the club of civil penalties--or fines--to go after those who don't honor their obligations under the law. So we are very supportive of strong data security legislation.

MS. SCHAKOWSKY. We have heard from a number of industries that the differences between significant and reasonable risk is a trigger from when notification should go out to consumers when their information is breached is itself significant. I wondered if you see the difference between the two as dramatically different.

MR. LEIBOWITZ. Speaking for myself, I think the most important thing, and again, this was actually a debate we had internally in the Commission when we made a recommendation, the most important thing is to have a trigger. You don't want every breach to require a notification to consumers because some breaches really don't raise any possibilities of harm.

From our perspective, we went back and forth and we came up with significant risk, and we think that is a pretty good standard. I don't see a whole lot of difference between significant risk and reasonable risk. They both have a trigger and they both seem, from my perspective at least, workable.

MS. SCHAKOWSKY. You may have said this already, but when do you think that the sale of Social Security numbers is good or useful, or is there a time?

MR. LEIBOWITZ. I think Social Security numbers have a lot of use in commerce and for commercial transactions. There are a lot of times when it involves credit, mortgages.

MS. SCHAKOWSKY. The sale of Social Security numbers?

MR. LEIBOWITZ. The sale of Social Security numbers? They have very legitimate uses in commercial transactions. Having said that, we also think they are overused and they are underprotected. So we look forward to working with you in trying to strike the appropriate balance, should you move legislation forward.

MS. SCHAKOWSKY. Great. I have no more questions. I can yield back.

MR. STEARNS. I thank the gentlewoman.
The gentleman from New Hampshire.

MR. BASS. No questions.

MR. STEARNS. Commissioner, I think you are all done, and so we will move to the second panel. But, of course, we have a vote here in 6 minutes, so we will take a temporary recess.

If the second panel will come forward, I think we have 2 or 3 votes and we will come back in a short amount of time. Thank you for your patience.

[Recess.]

MR. STEARNS. The subcommittee come to order. I want to thank you for your patience for waiting. And we thought that there weren't that many votes, but it turned out there were.

So from the second panel, Mr. Oliver I. Ireland, Partner with Morrison & Foerster; Ms. Susan McDonald, President of Pension Benefit Information; Ms. Lauren Steinfeld, former Associate Chief Counsel, Office of OMB; H. Randy Lively, Jr., President and CEO of American

Financial Services Association; and Mr. Marc Rotenberg, Executive Director of Electronic Privacy Information Center.

I don't know if you have your mike on.

STATEMENTS OF OLIVER I. IRELAND, PARTNER, MORRISON & FOERSTER, LLP, ON BEHALF OF FINANCIAL SERVICES COORDINATING COUNCIL; SUSAN McDONALD, PRESIDENT, PENSION BENEFIT INFORMATION; LAUREN STEINFELD, FORMER ASSOCIATE CHIEF COUNSELOR, OFFICE OF MANAGEMENT AND BUDGET; H. RANDY LIVELY, JR., PRESIDENT AND CEO, AMERICAN FINANCIAL SERVICES ASSOCIATION; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

MR. IRELAND. Here it is. I am here today on behalf of the Financial Services Coordinating Council, whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. The FSCC represents the largest and most diverse group of financial institutions in the United States, consisting of thousands of banks, insurance companies, and investment companies and securities firms that collectively provide financial services to virtually every household in the United States.

The FSCC appreciates the opportunity to be here today to discuss the use of Social Security numbers. Financial institutions work hard to protect the confidentiality and security of Social Security numbers. While the FSCC recognizes that misuses of Social Security numbers have occurred, we believe that it is imperative to avoid restricting necessary and appropriate uses of Social Security numbers by financial institutions since they have become critically important to our efficient and cost-effective financial system.

Financial institutions use Social Security numbers as a unique identifier for individuals. Broad restrictions on the use of Social Security numbers would have serious unintended consequences. Further, there are already substantial protections for the use of Social Security numbers by financial institutions.

Financial institutions do not make Social Security numbers accessible to the general public. They use Social Security numbers to combat fraud and identity theft; to assess underwriting risk, administer benefits, identify money laundering and terrorist financing, comply with Federal and State tax and securities laws; to transfer assets and accounts;

to comply with deadbeat spouse laws; to verify DMV records for auto insurance; to obtain medical information used for underwriting life, disability income and long-term care insurance; to locate missing insurance beneficiaries; and to locate lost insurance policies.

As the Government Accountability Office has recognized, the uniqueness and broad applicability of the Social Security number has made it the identifier of choice for government agencies and private businesses, both for compliance with Federal and State law and for business and administrative purposes. The use of Social Security numbers have become woven into the fabric of both government and commercial transactions in this country.

The FSCC is concerned about the potential consequences of a broad restriction on the use of Social Security numbers. As I have already noted, a broad restriction on the use of Social Security numbers could seriously impede the delivery of important financial services and the battle against criminal activity. For example, Social Security numbers are key for fraud detection. Without a unique common identifier such as a Social Security number, we believe that identity theft ultimately would be easier, not more difficult.

Further, the FSCC believes that there is no need to further restrict the use of Social Security numbers by financial institutions, given the strong Social Security number restrictions applied to these institutions under the Gramm-Leach-Bliley Act and other laws. For example, the Gramm-Leach-Bliley Act requires financial institutions to protect the security of their numbers, their customers' Social Security numbers, and, subject to exceptions for legitimate business purposes, each customer has a right to block a financial institution from transferring his or her Social Security number to a nonaffiliated third party.

In addition, this committee and other committees of Congress recently have passed additional requirements that would protect Social Security numbers at financial institutions and other institutions.

Thank you for the opportunity to be here today, and I will be happy to respond to any questions the committee may have.

MR. STEARNS. I thank you.

[The prepared statement of Oliver I. Ireland follows:]

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

I am Oliver Ireland with Morrison & Foerster LLP testifying on behalf of the Financial Services Coordinating Council ("FSCC"), whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. The FSCC represents the largest and most diverse group of financial institutions in the United States, consisting of thousands of large and small banks, insurance companies, investment companies, and securities

firms. Together, these financial institutions provide financial services to virtually every household in the United States.

The FSCC very much appreciates the opportunity to submit this statement to the Subcommittee concerning the use and misuse of Social Security numbers (“SSNs”). Our comments focus on the integral role of SSNs in United States commerce; the many consumer benefits that result from the use of SSNs by financial institutions; and the potentially negative effects that could occur if undue restrictions are imposed on such use. While the FSCC recognizes that there have been misuses of SSNs, we strongly urge that any legislation intended to address this problem be carefully targeted to specifically identified abuses, such as measures to stop identity theft. We believe it is imperative to avoid restrictions on legitimate and beneficial uses of SSNs.

Our testimony today focuses on three fundamental points:

- **First**, following the lead of the U.S. Government for the last 65 years, businesses have legitimately used the SSN as a unique identifier of individuals, and this use is now woven into the fabric of consumer and commercial transactions throughout the country. Moreover, this legitimate use of SSNs has produced real benefits for American consumers and taxpayers, and has become critically important for a wide range of government agencies, financial institutions, hospitals, blood banks, and many other businesses, both large and small.
- **Second**, broad restrictions on the use of SSNs could have serious unintended consequences, including: higher credit costs; increased fraud and identity theft; fundamental and costly changes to internal business operating systems; decreased consumer service; and costly delays in consumer and commercial transactions. Further restrictions on the use of SSNs may also impede law enforcement purposes, including with respect to money laundering and terrorist financing.
- **Third**, Congress has enacted privacy and information security protections under the Gramm-Leach-Bliley Act (“GLBA”) that, among other things, subject financial institutions to an affirmative and continuing obligation to protect the security and confidentiality of their customer’s nonpublic personal information, including SSNs, and establish stringent requirements for financial institutions concerning the use, transfer and protection of SSNs. In addition, more than 20 states have adopted statutes designed to protect the confidentiality of SSNs. Further, state security breach notification laws in some 30 states provide additional incentives to protect SSNs. Moreover, this Committee and other Committees of Congress recently have passed express requirements that would protect the security of SSNs. In light of these current and proposed protections, the FSCC strongly believes that further legislative restrictions on the use and transfer of SSNs by financial institutions are unnecessary.

Our statement also discusses the potentially negative impact of SSN restrictions on the legitimate use by financial institutions of public records.

As the Subcommittee is aware, Congress adopted privacy protections as part of the GLBA. The GLBA subjects the financial services industry to a comprehensive privacy framework that requires the annual disclosure of a financial institution’s privacy policies, allows customers to direct the institution not to share their “nonpublic personal information” with nonaffiliated third parties, contains significant prohibitions on the disclosure of detailed account information, and establishes regulatory standards to protect the security of “nonpublic personal information.” *Importantly, under the GLBA, SSNs are considered “nonpublic personal information,” and thus are already subject to significant restrictions on the transfer of, and the ability of others to reuse, such information.* Moreover, in 2003, Congress enacted additional legislation addressing concerns over identity theft, as part of its passage of the “Fair and Accurate Credit

Transactions Act of 2003.” These two Congressional initiatives go straight to the heart of Congressional concerns over identity theft and the efforts of financial institutions to combat this growing problem. In addition, the Committee on Energy and Commerce and other Committees of Congress recently have passed express requirements that would protect the security of SSNs.

As a practical matter, we do not believe that the financial services industry is the subject of the concern that Congressional legislation would attempt to address. We use SSNs, as well as other personal financial information, to assist us in making sound credit decisions, underwriting applications for insurance coverage and performing other ordinary insurance business functions, combating fraud, rooting out identity theft, and uncovering financial support for terrorism. We do not make SSNs accessible to the general public. As a result, we believe that any legislation should be targeted at those entities at the heart of the problem, be they unregulated information brokers, those engaged in illegal pretext-calling, or the like.

Integral Role of Social Security Numbers in U.S. Commercial Activities

To assist the Subcommittee in its deliberations, it may be helpful to review the important role that SSNs play in U.S. commercial activities.

As the Government Accountability Office (GAO) noted in a February 1999 report,¹ the Social Security Administration created the SSN in 1935 as a means to maintain individual earnings records for the purposes of that program. But, Congress soon realized the tremendous value to society of a unique identifier that is common to nearly every American. As a result, it began to require federal government use of the SSN as a common unique identifier for a broad range of wholly unrelated purposes and programs. For example, “a number of federal laws and regulations require the use of the SSN as an individual’s identifier to facilitate automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both.”² These include federal laws applicable to tax reporting, food stamps, Medicaid, Supplemental Security Income, and Child Support Enforcement, among others. Moreover, as the GAO acknowledged, it has repeatedly recommended in numerous reports that the federal government use SSNs as a unique identifier to reduce fraud and abuse in federal benefits programs.³

Following the federal government’s lead, American businesses complied with federal requirements to use SSNs as identifiers for federal laws unrelated to Social Security, such as income tax reporting. In doing so, they also realized the powerful consumer benefits to be derived from comparable business use of SSNs as a common unique identifier. Thus, businesses began to use SSNs in a manner similar to the federal government, *e.g.*, to match records with other organizations to carry out data exchanges for such legitimate business purposes as transferring and locating assets, tracking patient care among multiple health care providers, and preventing fraud and identity theft. Many businesses also use SSNs as an efficient unique identifier for such internal activities as identifying income tax filers.

Similarly, the financial services industry has used the SSN for many decades for a broad range of responsible purposes that benefit consumers and the economy. For example, our nation’s remarkably efficient credit reporting system—which has helped make America’s affordable and accessible credit the envy of the world—relies fundamentally on the SSN as a common identifier to compile disparate information from many different sources into a single, reliable credit file for a given consumer. Indeed, the

¹ “Social Security – Government and Commercial Use of the Social Security Number is Widespread,” February 1999, GAO/HEHS-99-28.

² *Id.* at 4.

³ *Id.*

banking, insurance, and securities industries each use SSNs for a variety of important regulatory and business transactions. Set forth below is an illustrative sample of the many financial institution uses of SSNs:

- To combat fraud and identity theft;
- To accurately assess underwriting risk;
- To assist in internal benefits tracking;
- To identify and report money laundering and terrorist financing activities;
- To comply with reporting requirements of federal and state tax and securities laws;
- To transfer assets and accounts to third parties;
- To comply with “deadbeat spouse” laws;
- To verify appropriate Department of Motor Vehicle records when underwriting auto insurance;
- To obtain medical information used in underwriting life, disability income, and long-term care insurance policies;
- To locate missing beneficiaries to pay insurance proceeds;
- To locate insurance policies for owners that have lost their policy numbers; and
- To facilitate a multitude of administrative functions.

As noted in the GAO report discussed above, “the uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies’ and businesses’ own purposes.”⁴ As a result, the use of SSNs as common unique identifiers has become woven into the very fabric of both government and commercial transactions in this country, and has been so for decades.

In short, the federal government began the use of SSNs for unrelated identification purposes; it required businesses to do the same under certain federal laws; and its use served as an example for businesses, including financial institutions, for over half a century. These uses have produced tremendous efficiencies and benefits for all Americans. The FSCC strongly urges members of Congress to keep such legitimate uses and benefits in the forefront when considering proposals to restrict the use of SSNs.

Unintended Consequences of Broad Restrictions on the Use of Social Security Numbers

As a result of the widespread use of SSNs for legitimate purposes, the FSCC is concerned about the potential unintended consequences of any legislation that is intended to restrict SSN abuses. If legislation is not carefully targeted to avoid these unintended consequences, consumers and the smooth operation of the U.S. economy could be seriously harmed. The following provides some specific examples of such harm:

- **Potential Harm to Consumers.** The use of SSNs allows financial institutions to provide a level of service to customers that would otherwise not be possible. By using these numbers to verify individual identities, credit bureaus and others can quickly provide financial institutions with accurate credit histories and verification information on people seeking credit, insurance, securities, and other financial products. In turn, a financial institution can act swiftly and efficiently on applications or requests related to these products. Use of SSNs also enables financial institutions to provide more seamless administrative service, including, for example, by allowing a life insurer to more easily verify the identity of an individual calling into a call center to change a beneficiary or premium mode or to make some other change to an insurance policy. The FSCC’s concern is that a broad restriction on the sale or use of SSNs, however

⁴ *Id.* at 2.

well-intended, could seriously impede the delivery of such important services by driving up processing costs and impairing decision-making.

- **Increased Risk of Fraud and Identity Theft.** SSNs are critical for fraud detection. Banks, insurance companies, and securities firms rely on information available from both public and private sources—with embedded SSNs to ensure correct identification—to check for “inconsistencies” that may suggest the occurrence of fraud or identity theft. The use of these numbers also helps financial institutions verify credit and other information necessary to make sound underwriting decisions that minimize losses. The sophisticated processes used for these purposes rely fundamentally on SSNs as the common unique identifier to assemble accurate and verifiable information for a given individual. That is, without a unique common identifier such as a SSN, we believe it would be *easier*, not harder, for an individual’s identity to be stolen. Thus, to reiterate, we believe that Congress should exercise great caution in restricting the use of SSNs so as not to risk an increase in consumer fraud or identity theft—a result that would be squarely at odds with the intended purpose of such restrictions.⁵
- **Market Disruption.** A prohibition on the sale of SSNs could be construed to restrict such activities as the sale of assets among financial institutions. This is so because financial institution assets (*e.g.*, mortgage servicing accounts, credit card accounts, and traditional bank accounts) often use SSNs as the basis for account identification. Also, SSNs are part of policy files that may be transferred by an insurer in connection with a merger or acquisition or as part of a reinsurance agreement. When it sells such an asset or transfers such files, a financial institution could be viewed as technically “selling” the embedded SSN as well. Thus, legislative efforts that “directly or indirectly” limit the transfer, sale, or purchase of SSNs could effectively preclude such plainly legitimate transactions. To address this problem, businesses would need to rework their internal systems completely to eliminate the reliance on such numbers—a massive and needless expense. Accordingly, we believe that any legislative proposal must be crafted to avoid such a significant, unintended consequence.
- **Money Laundering and Terrorist Financing.** Rules implementing section 326 of the USA PATRIOT Act require many financial institutions to obtain a taxpayer identification number, typically a SSN, before opening an account for the individual. The financial institution also must verify the identity of the individual. The verification process is facilitated by the use of SSNs. The section 326 requirement was adopted as part of comprehensive legislation to address terrorism following September 11, 2001. Any limitations on the use of SSNs would need to accommodate the section 326 information collection and verification processes.

Current Protections for Social Security Numbers

The FSCC believes there is no need to further restrict the use of SSNs by *financial institutions* in light of the strong SSN restrictions that apply to such institutions under the GLBA and other laws. The GLBA and its implementing regulations treat a financial

⁵ Existing law already includes provisions that prohibit identity theft. For example, stealing someone’s identity is punishable by civil and criminal penalties. *See, e.g.*, 18 U.S.C. § 1028. Moreover, the GLBA bans pretext calling—a tool of identity thieves.

institution customer's SSN as protected "nonpublic personal information."⁶ As a result, each financial institution is subject to an affirmative and continuing obligation to protect the security of its customers' SSNs, and each customer has the right to block a financial institution from selling or transferring his or her SSN to a nonaffiliated third party or the general public.

There are exceptions to this general rule for legitimate transfers of SSNs, such as ones that are necessary: to carry out a transaction requested by the consumer; to protect against fraud; and to provide necessary identifying information to credit bureaus. *However, even with respect to such legitimate transfers of SSNs, the consumer remains protected because the recipient of the number is prohibited by law from re-using or re-disclosing the number—it may do so only as necessary to carry out the purpose of the exception under which the number was received from the financial institution.* Further, the GLBA also requires financial institutions to establish appropriate safeguards to ensure the security of, and to protect against unauthorized access to or use of, SSNs.

In addition, more than 20 states have adopted statutes designed to protect the confidentiality of SSNs. For example, several states have enacted laws that prohibit specified uses of SSNs, including, for example, prohibiting the public display of a SSN. In addition, several states have enacted laws that limit the use of SSNs by state departments and agencies. Further, 30 states have enacted security breach notification laws. These laws generally require a business to notify consumers when a security breach occurs involving sensitive personal information relating to those consumers, including SSNs. Moreover, the Committee on Energy and Commerce and other Committees of Congress recently have passed express requirements that would protect the security of SSNs.

The existing and proposed federal and state protections for SSNs create strong incentives for financial institutions to protect the SSNs that they maintain. In light of these existing and proposed protections, and the corresponding incentives of financial institutions, the FSCC strongly believes that further legislative restrictions on the use and transfer of SSNs by financial institutions are unnecessary.

Concerns Over Restrictions On Access to Public Records

Finally, some concerns have also been expressed regarding the inappropriate use of SSNs available in the public record. The FSCC believes it is important to remember that a wide range of private sector enterprises—including banks, insurance companies, and securities firms—rely on these records to conduct a broad range of legitimate business activities. For example, financial institutions use public records to:

- Uncover fraud and identity theft;
- Make sound credit and other financial product determinations;
- Verify identities of the customer at the account opening phase;
- Assist in internal security operations (*e.g.*, employee background checks); and
- Otherwise verify identities in order to conduct a broad range of business transactions.

Business reliance upon public records facilitates the efficient operation of the financial and credit markets, limits mistakes, and ensures that consumers receive prompt and lower-cost service. It also helps protect the customer from fraud.

More specifically, to achieve the purposes described above, financial institutions directly use: public records involving liens on real estate; criminal records and fraud detection databases; and similar types of public records. Financial institutions also indirectly use these records for the same purposes by relying on databases developed by

⁶ *See, e.g.*, 12 C.F.R. § 40.3(o). The regulation generally defines protected "personally identifiable financial information" to include "any information . . . [t]he bank . . . obtains about a consumer in connection with providing a financial product or service to that consumers." *Id.* (emphasis added).

third parties that themselves rely on information from public records. Importantly, SSN identifiers are central to ensuring that the information included in these records matches the correct individual. This allows banks, for example, to verify the identity of a person so that a direction from a customer to transfer funds to a third party can be executed without mistake, as well as to check important credit-related characteristics of loan applicants (such as pending bankruptcies, tax liens, or other credit problems).

Moreover, financial institutions employ sophisticated programs that cross-check public information against information supplied by an applicant in order to uncover fraud. For example, if the age information provided by an applicant posing as another individual were inconsistent with other information known about that individual from public records made available through SSN identification, a “red flag” would be raised, which would trigger further checking to uncover the identity theft.

Thus, overly-broad limits on access to public record information would compromise a financial institution’s ability to make sound business decisions and to protect its customers. Such limits could also greatly slow the decision-making process of U.S. businesses, to the detriment of consumers and the economy. For example, if a SSN were stricken from a public record, it is possible that the ability to use that record for legitimate purposes would become impractical because of the expense involved in verifying the identity of the person covered by that record. The consequences could include delayed loan approvals, increased consumer costs for products and services, and limits on an institution’s ability to discover identity theft on a timely basis.

Even if public entities could still retain SSNs in their internal nonpublic files and financial institutions could obtain access to such files, the cost and delays in efficiently accessing such files would be significant. Ultimately, the cost efficiencies and speed of delivery inherent in our current market system would be compromised. The effect could be the same as denying financial institutions access to such records.

Conclusion

The benefits to society from the legitimate and responsible use of SSNs are real and substantial. As a result, the FSCC believes that policymakers should look carefully at the unintended consequences that could occur with any proposal that would restrict the use of these numbers. And, because of the existing restrictions on financial institution disclosure of SSNs, including the GLBA, we believe that no new SSN restrictions are required for the financial services industry.

MR. STEARNS. Ms. McDonald. Pull the mic up, and just turn it on, if you could.

MS. MCDONALD. Good afternoon, Mr. Chairman, and thank you for the opportunity to appear before your subcommittee as it reconciles the beneficial uses of SSNs with threats to privacy.

My name is Susan McDonald, and I am the President of Pension Benefit Information, otherwise known as PBI. For over 26 years PBI has provided research services to the pension industry. We assist sponsors of pension plans in fulfilling their fiduciary responsibility to manage their plans under the Employee Retirement Income Security Act of 1974, ERISA. PBI also supports pension plans in maintaining their qualified status. IRS regulations require minimum distributions to planned participants or their beneficiaries for that purpose.

Our services allow planned sponsors to ensure benefits get distributed to eligible participants. Our clients would be severely

impacted by an enactment of legislation that would restrict PBI from purchasing SSNs for the purposes of matching and retrieval. Such legislative restrictions would have serious consequences on millions of Americans that have earned benefits from their years of employment. Our clients typically come to us after they have performed a mailing, and it has come back undeliverable.

We serve over 9,000 planned sponsors in every industry segment. One of the greatest challenges for pension administrators is staying in contact with terminated vested participants. These participants are entitled to benefits, but are no longer employed by the company. They often forget to keep their address up to date and typically don't think about their benefits until they are nearing retirement age. By that time it can be hard to track down their pension, especially if the company has been sold or closed up shop decades ago.

A recent Boston Globe article outlined a widow's 6 year journey to track down her deceased husband's benefits. Most would have simply given up. Although it is hard to comprehend, every week PBI locates participants who had no idea they were entitled to benefits.

PBI retrieves our address information for participants based on their SSN. Maintaining accurate pension records is certainly a challenge since they have to maintain for so many decades, from the time a participant starts employment until their beneficiary dies. A lot can happen to lose contact with participants over that time. The companies we serve have migrated from 3-by-5 cards to keypunch cards and now to multiple system conversions. Records can and do get corrupted. Clients come to PBI because they are missing Social Security numbers or dates of birth for participants, or they have a beneficiary with no SSN.

PBI is currently able to perform research to identify a SSN so that a search for a participant can be made. The challenge of locating a female participant that could have changed her last name several times due to marriage or divorce would become nearly impossible if it were unable to utilize an SSN for research purposes.

To date we have located over 900,000 lost participants with their retirement benefits.

We support greater security and restriction for companies that are given access to information containing SSNs. Simply faxing a business license and checking a box to indicate a search for beneficial interests should not be deemed sufficient. This has been clearly demonstrated by several security breaches involving bogus accounts. As a consumer, this keeps me up at night.

PBI's primary data source for locate services is one of the three credit reporting agencies. We have established a long-term relationship

with them, meet on a regular basis, and they understand the services we provide and our customer base.

My desire in this testimony is to set forth the positive use of SSNs. We believe that our business is a prime example of how the use of SSNs yields socially beneficial results. Many of the people we help are older Americans who desperately need their pension benefits no matter how small or large.

With so many people changing jobs today, the task of locating former employees is becoming extremely difficult. They also change jobs. After they have changed their jobs, there are other issues associated with locating them as well. If we were not able to use the SSN, someone leaving out the middle initial or going by Bill versus William on employment documents would make it extremely difficult to locate them.

We currently locate 80 to 90 percent of the participants we look for using a SSN. If PBI is unable to utilize an SSN to research and retrieve addresses, our locate business would be in jeopardy. We search for participants nationwide and believe our results would be less than 8 percent if we could only use a participant's name. The chances of us ever finding the correct John Smith who worked for a particular employer would be nonexistent.

Our current process provides a cost-effective and efficient way to reunite former workers with their benefits. I doubt PBI could continue to provide our valuable service with diminished results and increased cost to validate we have located the right person.

We serve the Fortune 500, labor unions, government agencies, and third-party administrators across the country. We are required for the financial sector to complete 50-plus-page questionnaires and have the appropriate policies and procedures regarding data security, and we feel that that should be something that other companies have to provide in order to get access to the data.

I have highlighted some of the participants that we have found, and many of these were unable to find their benefits on their own, females that have changed their names. There are a lot of beneficial reasons that we perform our services, and feel that if we were unable to do the searches based upon that information, we would not be able to serve the constituents that you probably really want to serve at this point. Thank you.

MR. STEARNS. Thank you.

[The prepared statement of Susan McDonald follows:]

PREPARED STATEMENT OF SUSAN McDONALD, PRESIDENT, PENSION BENEFIT INFORMATION

Good afternoon Mr. Chairman and thank you for the opportunity to appear before your Subcommittee as it reconciles the beneficial uses of Social Security Numbers (SSNs) with threats to privacy. My name is Susan McDonald, and I am the President of Pension Benefit Information, otherwise known as PBI. For over 26 years PBI has provided research services to the pension industry. We assist sponsors of pension plans in fulfilling their fiduciary responsibility to manage their plans under the Employee Retirement Income Security Act of 1974, ERISA. PBI also supports pension plans in maintaining their qualified status. IRS regulations require minimum distributions to plan participants, and PBI locate participants, or their beneficiaries, for that purpose.

Our services allow plan sponsors to ensure pension benefits are distributed to eligible participants or their beneficiaries. Our clients would be severely impacted by the enactment of legislation that would restrict PBI from purchasing SSNs for the purposes of matching and retrieval. Such legislative restrictions would have serious consequences for millions of Americans who have earned benefits from their years of employment. Clients typically come to PBI after they have performed an ERISA mandated mailing, and communications come back undeliverable.

PBI serves over 9,000 plan sponsors in every industry segment. One of the greatest challenges for pension administrators is staying in contact with terminated vested participants. These participants are entitled to benefits, but are no longer employed by the company. They often forget to keep their address up to date, and typically don't think about their benefits until they're nearing retirement age. By that time it can be hard to track down their pension, especially if the company has been sold or closed up shop decades ago. A recent Boston Globe article outlined a widow's 6 year journey to track down her deceased husband's benefits, most would have simply given up. Although it's difficult to comprehend, every week PBI locates participants who had no idea they were entitled to benefits.

PBI retrieves address information for participants based upon their SSN. Maintaining accurate pension records is a challenge, since these records must be maintained for several decades. From the time a participant starts employment, until their beneficiary dies. A lot can happen to lose contact with participants over that time span. Companies have migrated from 3-by-5 cards, to keypunch cards, and now through multiple system conversions. Records can, and do get corrupted. Clients come to PBI because they are missing Social Security Numbers or Dates of Birth for participants. Or, they have the name of a beneficiary with no SSN. PBI is currently able to perform research to identify a SSN so that a search for a lost participant or beneficiary can take place. The challenge of locating a female participant, that could have changed their last name multiple times due to marriage or divorce, would become nearly impossible if we were unable to utilize a SSN for research purposes.

PBI's address location service is designed to meet the requirements of the Pension Benefit Guaranty Corporation (PBGC) to perform a "diligent" search. The PBGC protects the retirement incomes for companies that have terminated their pension plans. The PBGC provides specific guidelines to administrators of terminating plans with regards to lost participants. Under the law, a search is considered diligent if it includes use of a commercial location service to search for the missing participants (29 CFR 4050.4). PBI performs this valuable service, and ERISA attorneys provide many of our referrals.

To date, PBI has reunited over 900,000 lost participants with their retirement benefits. We don't simply provide an address retrieved from a database. We communicate an important message to lost participants, and the lost participant confirms their address to PBI. Clients look to PBI to perform our diligent search process, since

many of them are ill equipped to manage returned mail. Our clients also want to demonstrate they've been prudent in fulfilling their responsibilities to participants.

PBI supports greater scrutiny and restrictions for companies that are given access to information containing SSNs. Simply faxing a business license and checking a box to indicate a search is for beneficial interest should not be deemed sufficient. This has been clearly demonstrated by several security breaches involving bogus accounts. As a consumer, this keeps me up at night! PBI's primary data source for locate services is one of the three credit reporting agencies. We've established a long term relationship with them, meet on a regular basis, and they understand the services we provide and our customer base. Due to the increase in data security breaches, along with the sophisticated phishing scams, consumers are fearful of disclosing any information. What used to be the simple confirmation of a correct address has raised concerns with lost participants. As a result, PBI's costs have sky-rocketed to provide our locate service.

My desire in this testimony is to set forth the positive uses of SSNs. We believe that our business is a prime example of how the use of SSNs yields socially beneficial results. Many of the people we help are older Americans, who desperately need their pension benefits, no matter how small or large. With so many people changing jobs today, the task of locating former employees is becoming increasingly difficult. Americans move on average every five years, particularly when they change jobs. They also often change their names with marriage or list slightly different names (*i.e.*, leave out a middle initial or use Bill versus William) on employment documents. If PBI was unable to utilize a SSN for retrieval purposes our results would plummet. We currently locate 80-90+% using a participant's SSN. If PBI is unable to utilize a SSN to research and retrieve addresses our locate business will be in jeopardy. We search for participants nationwide, and believe our results would be less than 8% if we could only use a participant's name. The chances of us ever finding the correct "John Smith", who worked for a particular employer, would be non-existent. Our current process provides a cost-effective and efficient way to reunite former workers with their benefits. I doubt PBI could continue to provide our valuable service with diminished results and increased costs to validate we've located the "right" person.

PBI serves the Fortune 500, labor unions, government agencies and third party administrators throughout the country. We also work with many of the largest financial and insurance companies. Our clients, especially those in the financial sector, demand that PBI have policies and procedures in place to protect confidential information. It's a pre-requisite for doing business with them. We are required to answer 50+ page questionnaires regarding data security, and provide documentation on our policies and procedures. Similarly, PBI requires clients to provide written authorization before we start a locate project. We only search for participants that are entitled to benefits. On occasion a client will come to us because they unintentionally overpaid a participant. We refer them to other services in those instances, since it violates our policy of "beneficial interest".

Our locate service is used for a variety of reasons. These include uncashed/stale dated checks, returned 1099 statements, notice of plan changes, eligibility to commence benefits, due a distribution, terminating plans, Summary Annual Reports, etc. One of the most recurring corporate events that contribute to lost participants is mergers and acquisitions ("M & A"). When an M & A activity takes place the pension assets usually move to the new company. This company is often in a new city, with a new corporate name. Individuals lose track of these occurrences and, thus, have obvious difficulties tracking down their vested benefits. As an example, PBI successfully located thousands of participants for a division of Westinghouse. This division of Westinghouse was acquired by CBS, and then CBS was acquired by Viacom. Now Viacom is in the process of splitting into two separate companies. How will participants know where to find their benefits in these types of situations?

Sometimes we locate individuals whose lives are changed dramatically by our use of SSN searches. For example, we recently located a disabled woman who worked decades ago for a grocery store that's no longer in business. She had been trying to track down her benefits for years, and was unsuccessful. PBI located her, and she was so happy to be found that she sent us a letter and included a check for \$20.00! We promptly returned her check, but this shows just how valuable a lost participant deems our service. In her letter to PBI she said "I have been married and divorced twice since then and have taken back my birth name." The chances of PBI locating her without an SSN is remote, just as her ability to locate her hard earned benefits on her own were.

Similarly, we were able to locate a 67 year old man who worked for a metal plating company for 25 years. He paid union dues and knew he was entitled to an annuity at retirement age. The company he worked for went bankrupt 16 years ago, and he was unable to locate his benefits. After he applied to the Social Security Administration at age 65, the SSA sent him a letter notifying him he was eligible for an annuity. An address was provided for him, and he thought his lost pension had been found. Wrong, when he arrived at the address provided no one was aware of his pension benefits. The only advice given to him was to hire an attorney. With a pending move to Texas, combined with fear over the fees involved in hiring an attorney, he gave up on ever finding his benefits. PBI located him on March 20th of this year, and he just received confirmation of his monthly annuity. Needless to say, he's ecstatic to be reunited with his benefits.

Last fall we assisted Shell Oil Company in locating several hundred employees that were unaccounted for due to Hurricanes Katrina and Rita. Shell discovered that many employees did not have emergency contact information on file, or if they did, they were in the same area impacted by poor telephone communications. We promptly went to work and provided them with valuable information to reach out to employee's relatives. Our contact at Shell was thrilled to notify PBI that all of Shell's employees were located and found safe. PBI provided valuable assistance to Shell under chaotic circumstances. Their employees were delighted to obtain housing assistance from their employer in their time of need.

As the above examples underscore, the ability to use SSNs for matching purposes in commercial databases is critical to our efforts to reunite former employees with their benefits. Without the ability to use an SSN, a slight misspelling in a name, the presence or absence of a middle initial, and a less distinctive name can drastically reduce a plans ability to locate pension fund beneficiaries. I'm urging you to carefully consider the beneficial reasons for having access to SSNs and request that provisions be put in place that allow exceptions for qualified businesses such as ours.

The Department of Labor (DOL) just finalized regulations for dealing with "orphaned" plans, or plans which have been abandoned by their sponsors. The regulations rely on a Qualified Termination Administrator to notify participants and distribute benefits. I can't imagine how this function will be performed for participants that have moved since their previous employment with a defunct company. In addition, terminating defined contribution plans, not insured by the PBGC, are required to distribute all funds by law. Plans are required to demonstrate their due diligence in attempting to locate participants, and PBI fulfills that purpose. If participants are not located the plan will need to take out an Individual Retirement Account (IRA) or annuity. Or, they can escheat the funds to the state's unclaimed property fund of the participant's last known address. I'm convinced the chances of a participant ever finding their account balances under these circumstances are slim to none. I believe these participants would be thrilled to be reunited with their account balances through our service.

Thank you, Mr. Chairman and Members of the Subcommittee, for the opportunity to express the views of Pension Benefit Information. I welcome the opportunity to provide additional information to you regarding this troublesome issue. My sincere desire is that future legislation will best serve and protect constituents while preserving privacy at the

same time. Legitimate business to business relationships must be preserved so that plan sponsors can fulfill their responsibilities under ERISA. Since PBI provides call center support to lost participants, I can tell you with confidence how grateful they are to be reunited with their benefits. I look forward to an opportunity to work with your committee to ensure the positive uses of Social Security Numbers continue to be protected.

MR. STEARNS. Ms. Steinfeld.

MS. STEINFELD. Good afternoon, Mr. Chairman. And thank you for the opportunity to speak before you about Social Security numbers and commerce, reconciling beneficial uses with threats to privacy.

My name is Lauren Steinfeld. I have worked on privacy generally at the Federal Trade Commission, on SSN legislation in my time at OMB, and I now work for the University of Pennsylvania as its Chief Privacy Officer. I'm testifying today on my own individual capacity and not on behalf of the University of Pennsylvania.

In my written testimony I discussed the risks and benefits of using SSNs, the positive direction of H.R. 1078 introduced by Representative Markey, and H.R. 1745 introduced by Representative Shaw, and I introduced certain comments on specific provisions in the bill.

Today I will discuss what I believe are the most important points. First and foremost, in my view, it is entirely appropriate to ban the uncontrolled sale and purchase of Social Security numbers. SSNs can be and are used by thieves to take out credit, to apply for insurance, and even to defraud the tax system. The abuse of Social Security numbers causes considerable harm to individual victims, to merchants who are not paid, and, ultimately, to honest consumers who bear the cost by paying more for credit. It is difficult for us to say that we, as a society, are sincerely working to curb the rising incidence of identity theft when Social Security numbers are lawfully for sale to anybody with an Internet connection.

Second, it is not appropriate to ban all sales and purchases of Social Security numbers. SSNs are the closest thing we have to a national identifier, and by helping to link the different sources, SSNs are often the key, when properly used, to many important commercial activities, to public health interventions, to medical research, to finding missing children, to locating fugitives from justice, and other law enforcement and national security imperatives.

The proper way to balance the risks and benefits of using Social Security numbers is to utilize the rulemaking process to allow for detailed analysis and careful crafting of exceptions based on public comment and agency expertise. H.R. 1078 and H.R. 1745 each include rulemaking provisions, but they differ in their assignment of rulemaking

authority. The former gives it to the FTC and the latter to the Attorney General.

I believe the rulemaking authority should go to the FTC for three reasons. One, the FTC, through its dedicated ID theft program, is well versed on the causes of identity theft and is in a solid position to address the privacy risks and overexposing SSNs. Two, the FTC has a deep understanding of the competing interests to SSN restriction through its long history of working with the data broker industry. Finally, the FTC, through its experience in promulgating the Safeguards Rule under the Gramm-Leach-Bliley Act, has now developed more technical expertise to better evaluate the burdens and benefits of securing the sensitive SSN.

Now I would like to focus on some provisions that appear in H.R. 1745. Several of them go far towards protecting privacy and involve very few trade-offs. These are the provisions restricting the display of SSNs on government checks and restricting the display of SSNs on employee ID cards from the Government and private sector.

H.R. 1745 also contains worthwhile reasonable measures to protect provisions that can offer strong advantages similar to those coming from the Gramm-Leach-Bliley rule.

I would like to raise the following point about Section 109. That section makes it unlawful to refuse to do business with an individual because that individual will not provide a Social Security number, and that provision is to be effective within 180 days. The provision could be problematic for some industries in this time frame, particularly health care where the SSNs may very well be the key to linking medical data for treatment purposes, coordination of benefits, and performing critical medical research.

In conclusion, there is ample room for optimism for greatly reducing risks that arise from the overavailability of Social Security numbers, and this is a critical effort and will remain so for as long as we have credit processes that allow for the extension of credit based on name, address, and Social Security number alone.

In the last several years, we have learned a great deal about workable models for protecting privacy, about compromising important other priorities. I applaud the authors of H.R. 1078 and H.R. 1745 for creating another good example of this in the important area of protecting SSNs.

I thank you for the opportunity to appear before you and welcome any questions you may have.

MR. STEARNS. Okay. Thank you.

[The prepared statement of Lauren B. Steinfeld follows:]

PREPARED STATEMENT OF LAUREN STEINFELD, FORMER ASSOCIATE CHIEF
COUNSELOR, OFFICE OF MANAGEMENT AND BUDGET

Good morning and thank you for the opportunity to speak before you today about Social Security Numbers in Commerce – Reconciling Beneficial Uses with Threats to Privacy. I am delighted to share some views on an issue about which I have thought for some time. In today’s testimony, I will describe some examples of the risks and benefits of using SSNs. I will also share my view that the two bills being considered by this Committee, H.R. 1078 and H.R. 1745, go far towards advancing privacy protection while also addressing important commercial, health, and safety concerns. Finally, I will offer some views on particular provisions in the bills.

My background on privacy issues is as follows. I began working at the Federal Trade Commission in 1995 where I was a staff attorney in the Division of Financial Practices and then in 1998 served as Attorney Advisor to Commissioner Mozelle Thompson. The following year, I became Associate Chief Counselor for Privacy, working for Peter Swire, the Chief Counselor for Privacy, at the Office of Management and Budget. In this role, I worked on a wide variety of privacy issues, two of which are especially relevant to this discussion: First, I served as the lead staff person to help develop proposed legislation regarding Social Security number protection – the Social Security Number Protection Act of 2000 was introduced by Representative Markey as H.R. 4611 and Senator Feinstein as S. 2699. Second, I was the coordinator within OMB for the report issued by OMB, the Department of Treasury and the Department of Justice entitled “Financial Privacy in Bankruptcy: A Case Study on Privacy in Public and Judicial Records.” Currently, I serve as Chief Privacy Officer for the University of Pennsylvania where I coordinate programs on a number of fronts to reduce SSN-related risks.

In today’s testimony, I am presenting my own views based on my experiences and not the views of the University of Pennsylvania, nor the views of the Clinton or Bush Administrations from my time at OMB.

The Risks and Benefits of SSNs

We, as a society, are struggling to get our arms around how to manage a small piece of data that can raise big problems and provide big benefits – that is, the Social Security number. The most common problem the SSN creates is that it can be used, indeed abused, by thieves, in combination with often other publicly available data, to commit identity theft. Often identity theft occurs in the following way: the thief starts by obtaining a limited amount of information about someone else and uses it to obtain credit, for example by opening a credit card account or cell phone account, in the victim’s name. The thief then runs up charges on the account and fails to pay those charges. The victim’s credit reports will show significant delinquencies that interfere with the victim’s ability to obtain a loan, a mortgage, insurance, even a job. In addition to damage to identity theft victims, identity theft also costs credit providers who are not paid amounts based on fraudulent charges. These costs are eventually largely borne by honest users of credit who pay more.

Another example of identity theft comes in the context of tax filings. A thief may use a legitimate taxpayer’s personal information to file a fraudulent tax return designed to provide a refund. Those thieves may then go on to take out “refund anticipation loans,” based on the amount they have “allowed themselves” in their filing. A recent New York Times article, based on an interview with an IRS official, reported that there were 8,000 instances in one year of information of legitimate taxpayers being used by imposters to try to defraud the tax system.

Identity theft is now the fastest growing crime in America, because of the ease with which it can be committed. It is so easy because the very limited information required to

open accounts is easily available. While name and address and even date of birth are often presumed to be public, it is the Social Security number that is intended to be the one key piece of private data that lets, for example, creditors know they are in fact extending credit to the person whom the applicant claims to be. When that Social Security number is not in fact private, a key foundation for the integrity of the credit granting system is compromised. I have heard anecdotally from a law enforcement officer that in the past, the conversation in prison yards centered on bank robbery. Now, the “buzz” is that bank robbery is too difficult; identity theft is the way to go.

It is tempting as a society to declare then that Social Security numbers should be banned except for purposes of administering the Social Security system and for tax-related purposes. But to shut down the use of Social Security numbers poses different, but also highly significant, problems.

Social Security numbers are the closest thing we have to a national identifier and, by helping to link different data sources, they are often the key to advancing national priorities. They facilitate important commercial activities, including the granting of loans, insurance and employment through the credit reporting system that – when working ideally – allows industry to judge an applicant according to information *about that applicant*. They help us gather critical public health data for investigations and sometimes life-saving interventions. They enable vital health-related research on individuals over time and over different health care settings. Social Security numbers help us locate missing children and fugitives from justice and generally provide crucial data for law enforcement and national security purposes.

Crafting Legislation

With the risks and the benefits of Social Security numbers largely understood, the challenge in crafting legislation is how best to tackle the privacy concerns, without creating the unintended consequences of hindering fraud detection, law enforcement, national security, research, and other significant priorities. In my personal opinion, the two bills being considered by the Committee strike the balance quite well in many respects.

Banning the Uncontrolled Sale and Purchase of SSNs

First and foremost, the bills would outlaw the uncontrolled sale and purchase of Social Security numbers. Today, it is lawful to create a website and offer SSNs for sale – regardless of who is asking and regardless of the purpose. In fact, one website I found advertises “Locate a Social Security number -- Supply a name & address or previous address, we will supply a social security number!” Another site says,

“The Internet is the largest information base in the world, and we have uncovered thousands of resources that will have you simply amazed ... and all of this is 100% legal.”

When working on SSN-related initiatives at the University of Pennsylvania, I have heard people remark that while we are spending great amounts of money, time, and effort to remove SSNs from our systems and documents, and to convert to what we call a “PennID,” it is frustrating to know that the SSNs we are protecting are literally “for sale” by others on the Internet. Legislation banning the uncontrolled sale or purchase of SSNs can help send a strong signal to organizations working to protect SSNs that their efforts are even that much more worthwhile.

As I stated above, the bills would outlaw the *uncontrolled* sale and purchase– but not *all* sales and purchases. That is appropriate to accommodate the critical beneficial uses of SSNs described above. Both H.R. 1078 and H.R. 1745 set out largely similar exceptions to the restrictions on the sale and purchase of SSNs. They allow, for example,

SSNs to be sold or purchased for law enforcement or national security purposes, for public health purposes, for emergency situations, to the extent necessary for research, and pursuant to consent – and each bill allows for further development of the exceptions in a subsequent rulemaking.

Differences in Approach to Rulemaking

A key difference in the bills lies in how that rulemaking will be conducted. H.R. 1078 gives the Federal Trade Commission authority to promulgate rules within one year regarding unfair or deceptive acts or practices in connection with the sale and purchase of SSNs – all in consultation with the Commissioner of Social Security, the Attorney General, and other agencies as the Commission deems appropriate. H.R. 1745 gives the rulemaking authority to the Attorney General, in consultation with the Commissioner of Social Security, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Secretary of the Treasury, the Federal Trade Commission, the Federal banking agencies, and National Credit Union Administration, the Securities and Exchange Commission, State attorneys general, and certain State insurance commissioners.

In my opinion, the Federal Trade Commission should be given the primary authority to issue regulations in this area for the following reasons:

- The FTC has significant expertise in understanding identity theft through the program it administers under the Identity Theft Assumption and Deterrence Act of 1998. In particular, the FTC is well versed on the causes of identity theft and is in a solid position to address the privacy risks in overexposing SSNs.
- The FTC also has a deep understanding of the competing interests to SSN restriction through its work with the data broker industry, first in helping to develop the industry self-regulatory program in the late 1990s and more recently in the aftermath of the Choicepoint breach.
- Finally, the FTC, through its experience in promulgating the Safeguards Rule under the Gramm-Leach-Bliley Act, is aware of the important difference between “reasonable safeguards” and “perfect security.” As a result, the FTC has now developed more technical expertise to evaluate burdens and benefits in securing the sensitive SSN.

While I believe the FTC expertise should be leveraged to the fullest advantage, I also believe that consultation with the agencies named in H.R. 1745 would provide additional controls to ensure that the many considerations of beneficial and risky uses are addressed.

As far as what the rulemaking should cover, I recommend that the bills contain an additional provision – the rulemaking agency should address the issue of verifying the identity and authority of requesters seeking SSNs under one of the enumerated exceptions. We have seen in the Choicepoint breach that a critical control to protecting privacy is adopting robust procedures to check the credentials of callers and writers claiming to be legitimate and to be using data for legitimate purposes. Today, certain websites are willing to furnish sensitive data such as Social Security number on the mere “I agree” click that I have a permissible purpose under the Fair Credit Reporting Act. It is worth considering the burdens and benefits of different verification approaches to provide reasonable assurances that requests truly are legitimate. Adding requirements in this area is important to realize the goals of the bills overall.

Additional Regulation in H.R. 1745

Another key difference between H.R. 1078 and H.R. 1745 is that the latter goes beyond restricting the sale and purchase of SSNs. H.R. 1745 reaches into many additional areas that are well worth acting upon and for the most part do not raise the same types of tradeoffs. The provisions dealing with public display of SSNs are especially valuable.

H.R. 1745 places special provisions on governmental agencies and prohibits them from displaying SSNs on checks issued for payment. For the public and private sector, the bill also prohibits placing SSNs on employee identification cards or tags. H.R. 1745 also prohibits inmate access to SSNs. These measures are entirely appropriate as a risk benefit matter, though one must recognize that even seemingly simple process changes, when applied so broadly, can take significant time and resources. I encourage the Committee to confirm the appropriate timeframe for instituting these measures.

H.R. 1745 also includes a requirement that both the public and the private sector adopt “measures to preclude the unauthorized disclosure of Social Security numbers.” The spirit of this provision seems very well aligned with the Safeguards Rule of the Gramm-Leach-Bliley Act. I encourage aligning the language of the bill more closely with the GLB Safeguards Rule and, again, vesting rulemaking authority with the Federal Trade Commission to help achieve that consistency.

One final point on H.R. 1745 concerns Section 109 – making it unlawful to refuse to do business with an individual because the individual will not provide a Social Security number – that provision being effective within 180 days. I suspect that this provision could be very problematic for some industries in this time frame, particularly health care, where the SSN may very well be the key to linking medical data for treatment purposes, coordinating benefits, and performing critical medical research. I encourage the Committee to review this provision and the timeframe more closely and to reach out to affected industries, before passing legislation. Alternatively, the impact of this provision could be researched and the language refined in a rulemaking as well.

Conclusion

There is ample room for optimism in greatly reducing risks arising from the overavailability of Social Security numbers. This is a critical effort and will remain so for as long as we have credit processes that allow for the extension of credit based on name, address, and Social Security number alone.

In the last several years, we have learned a great deal about workable models for protecting privacy without compromising important other priorities. For example, I described above the work of OMB, the Department of Treasury and the Department of Justice on “Financial Privacy in Bankruptcy: A Case Study on Privacy In Public and Judicial Records.” That report recommended what I believe to be a balanced model in which full bankruptcy case files are available to “real parties in interest,” to enable them to protect their rights, while the general public would be restricted from certain sensitive data, like Social Security numbers and bank account numbers, that are not necessary for the public to know in the name of accountability of the bankruptcy system. In this example, combined with many others, we have learned that privacy and accountability – or commerce or national security as the case may be -- may be spoken in the same sentence and often do one another a service. When stakeholders from all vantage points work in earnest on crafting a better data confidentiality model – all are better off.

My optimism is confirmed by the authors of the two bills before the Committee who recognize that the time has come for a consensus to prohibit the uncontrolled sale and purchase of the highly sensitive Social Security number. I am pleased that the authors are finding ways to take important steps to protect privacy while also protecting other critical goals. I thank you for the opportunity to appear before you and welcome any questions you may have.

MR. STEARNS. Mr. Lively.

MR. LIVELY. Thank you, Mr. Chairman. Good afternoon. My name is Randy Lively. I am the president and CEO of the American Financial Services Association here in Washington. AFSA’s 300-member

companies include consumer and commercial finance companies, captive auto finance companies, credit card issuers, mortgage lenders, and other financial service firms that lend to consumers and small businesses.

I am pleased to be here today to discuss the importance of the Social Security number for our member companies. While Social Security numbers are not the sole identifier used by the financial services companies, they are critically important to our industry for a couple of reasons. First, they provide a unique means of identity verification, and second, they are an essential component of the industry's system to detect fraud.

The Social Security number itself acts as an identity verification. It provides a unique identifier that accompanies most consumers throughout their lifetime. This number remains consistent in a world where people's names and addresses are changing constantly, whether for marriage, divorce, or, in the case of people moving from State to State, the reissuance of driver's licenses.

Financial services companies use Social Security numbers to help ensure the accurate association of financial accounts, credit reports, public records, medical records, and other relationships or services to a consumer. A company typically uses the Social Security number or subsets of the number internally to track a customer's relationship with that company across multiple accounts and for other legitimate reasons.

For a financial services company, a Social Security number plays a pivotal role in identity determination. In particular, it allows companies to establish and verify the identity of people with whom the institution conducts business.

With millions of John Smiths in America, a financial services company needs a way to determine which John Smith is its customer. It does this with the help of a unique identifier common to all Americans, the Social Security number. Importantly, financial services companies realize that the ability to successfully verify John Smith's Social Security number is not the same as successfully determining his identity. To do this, a company uses a driver's license, passport, or another government-issued identification document with a picture, signature, expiration date, security features, and a physical description and so forth.

It is worth noting that the Social Security number has not been used solely for identity verification due to the lack of a highly secure Social Security number card with a tamper-proof signature, picture, and expiration date. The Social Security number card contains few security features, thus making it easy to counterfeit. The Social Security number is only a tool, albeit an invaluable one, in the process of determining the identity of an individual. It is clear, however, that verification is a key tool for achieving positive identity determination.

The issue of fraud, according to the Federal Trade Commission, identity theft robs the Nation of more than \$50 billion annually. Consumer losses account for about \$5 billion of that, and of the total, the business community absorbs the remaining \$45 billion. The availability of the Social Security number both in the financial services companies' database and in public records is essential for law enforcement officials during a criminal investigation. The number provides the most reliable method to identify and associate perpetrators to their public records which often provide details needed to solve the crime.

What is more, the Social Security number is critical in verifying a potential employee's background and allows for the ongoing monitoring of employees in high-risk positions. Without the use of a Social Security number, financial services companies would find it very difficult to adhere to a know-your-employee standard.

To keep the trust of valued customers, AFSA companies take every precaution to protect their customers' Social Security numbers and other personal financial information. This an ongoing employee training in the handling of sensitive personal information. It also includes close scrutiny of the practices of third-party vendors who store or dispose of data which may contain personal financial information.

The industry has worked hard to put mechanisms in place to ensure security breaches are rare. Just as this is important to law enforcement and legislators, it is also critical to the financial services industry so it has customers who are safe, content, and desirous to do business with its companies.

In conclusion, as we explore ways to protect consumers' privacy, we should take care to thoroughly evaluate any proposed restrictions on the use, sale and purchase of Social Security numbers to ensure that unintended consequences do not occur.

Thank you, Mr. Chairman.

MR. STEARNS. Thank you.

[The prepared statement of H. Randy Lively, Jr., follows:]

PREPARED STATEMENT OF H. RANDY LIVELY, JR., PRESIDENT AND CEO, AMERICAN
FINANCIAL SERVICES ASSOCIATION

Mr. Chairman, my name is Randy Lively and I am the President and CEO of the American Financial Services Association located here in Washington, DC.

AFSA's 300 member companies include consumer and commercial finance companies, "captive" auto finance companies, credit card issuers, mortgage lenders and other financial service firms that lend to consumers and small businesses. This year, AFSA is celebrating its 90th birthday as the nation's premiere consumer and commercial credit association.

I am pleased to testify here today on the importance of the Social Security Number for our member companies in the auto finance, mortgage finance, credit card and personal loan lines of business. While Social Security Numbers are not the sole identifier

used by financial services companies, they are critically important to our industry for a couple of reasons. First, they provide a unique means of identity verification. And second, they are an essential component for the credit industry's systems designed to detect and prevent fraud. Let's look at these one at a time.

I. Social Security Numbers – A Unique Means of Identification

The Social Security Number provides a unique identifier that accompanies most consumers from cradle to grave. This number remains a constant in a world where people's names and addresses are constantly changing -- whether from marriage, divorce, addresses, or driver's license re-issuance as consumers move from one state to another.

Financial services companies use Social Security Numbers to help ensure the accurate association of financial accounts, credit reports, public records, medical records and a host of other critical relationships and services to a consumer. A company typically uses the Social Security Number (or subsets of the number) internally to track a customer's relationship with that company across multiple accounts and for other legitimate internal reasons.

For a financial services company, a Social Security Number plays a pivotal role in identity determination. In particular, it allows companies to establish and verify the identity of unique persons with whom the institution, and others, conduct business. With millions of John Smiths in America, the identity determinate of which John Smith with whom a finance company is dealing is made by the single unique identifier common to all Americans, his Social Security number.

Importantly, financial services companies realize that the ability to successfully verify John Smith's Social Security Number is not the same as successfully determining his identity. A company must do this by using a driver's license, passport or another government-issued, identification document containing a picture, signature, expiration date, security features, a physical description, etc.

It's worth noting that Social Security Numbers have not been used solely for identity verification due to the lack of a highly secure Social Security Number card, tamper-proof signature, picture and expiration. The Social Security Number card contains few security features, making it easy to counterfeit thus reducing or eliminating any value in its sole use for identity verification. The Social Security Number is thus only a tool, albeit an invaluable one, in the process of determining the identity of an individual. It is clear, however, that verification is a key tool for achieving positive identity determination.

II. Social Security Numbers – An Essential Component of the Industry's Ability to Detect Fraud

According to the Federal Trade Commission, identity theft robs the nation of more than \$50 billion annually. Consumer losses account for about \$5 billion of the total and business absorbs the remaining \$45 billion.

The availability of the Social Security Number both in the financial services company's database and in public records is essential for law enforcement officials during a criminal investigation. This number is the most reliable method of identification, correlation and association of the perpetrators to their public records, which often provide critical details imperative to solving the crime and locating the suspect(s). The loss of this valuable tool would jeopardize the effective investigation of financial crimes.

What's more, the Social Security Number is critical in verifying a potential employee's background and allows for the ongoing monitoring of employees in high-risk positions. Without the use of a Social Security Number, financial services companies would find it very difficult to adhere to a "know your employee" standard.

To earn and keep the trust of valued customers, AFSA companies take every precaution to protect their customers' Social Security Numbers and other personal

financial information. This includes on-going training for employees in the handling of sensitive personal information. It also includes close scrutiny of the practices of third-party vendors who store or dispose of data which may contain personal financial information. The industry has worked hard to put mechanisms in place to ensure security breaches are rare. Just as this is important to law enforcement and legislators, it is also critical to the financial services industry, so we have customers who are safe, content and desirous to do business with our companies.

Conclusion:

AFSA member companies share this committee's goal of wanting to assure American consumers that their personal information, including their Social Security Number, is safely protected. At the same time, we must be mindful that many financial services companies utilize the Social Security Number internally for a variety of legitimate business reasons, which should remain exempt from additional limitations.

As we explore ways to protect consumers' privacy, we should take care to thoroughly evaluate any proposed restrictions on the use, sale and purchase of Social Security numbers to ensure that unintended consequences do not occur.

Obviously, the best way to protect our customers' information is to prevent fraud from occurring in the first instance. Through the kinds of methods I just described – such as employee training of the handling of sensitive information, and close scrutiny of third-party vendors – the industry is committed to doing its part.

Finally, it worth mentioning the role of the customer. Consumers who are proactive and understand the importance of safeguarding their Social Security Number can serve as the first line of defense in preventing fraud.

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

MR. STEARNS. Mr. Rotenberg.

MR. ROTENBERG. Thank you, Mr. Chairman. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center. I appreciate the opportunity to be before the subcommittee today, to see you again, and to talk about the Social Security number issue. I would like to ask that my written statement be entered.

MR. STEARNS. By unanimous consent, so ordered.

MR. ROTENBERG. I would like to make a few brief comments. I know it is late in the day. I think this is a very important hearing that you are holding. The risks of the misuse of the Social Security number in the United States, I think, are widely shared by American consumers. There has been a dramatic increase in the incidence of identity theft in this country. It imposes a real economic hardship, and it has been closely linked to the use of the Social Security number in the private sector.

Now, I would like to describe two of the types of problems that arise for consumers when their Social Security numbers become available to others. The first, as you may know, is that many financial institutions use the Social Security number both as an account locator and as the password on the account, so that, in effect, if you have a person's Social Security number, you have the ability to access the contents of that

financial account, which is why it is so attractive to identity thieves. It is literally the keys to the kingdom. The Social Security number also makes it possible to link together records from different sources and to build profiles.

Now, it is true in terms of investigating a financial fraud and making credit determinations that it plays an important role in the private sector, and we understand that. But at the same time, it also opens the door to a kind of open-ended profiling of American consumers that makes the work of identity thieves that much easier.

Now, the interesting thing about this particular issue is that Congress understood the problem, both in the creation of the number when the Social Security agency said, we are going to limit the use of the number so that it is only used for the SSA purposes, and again in 1974 when the Comprehensive Privacy Act passed on a bipartisan basis, said to the Federal agencies, we really want to limit the use of the Social Security number.

Now, I actually went back the other day and looked at the history of the 1974 act and found something very interesting. It was an important report that provided the basis for that act, and that report said specifically that legislation should be adopted, and I am quoting now, it is in my statement, "prohibiting uses of an SSN or any number represented as an SSN for promotional or commercial purposes." The Senate report that accompanied passage of the Privacy Act said, in 1974, the use of the Social Security number in the private sector is, quote, "one of the most serious manifestations of privacy concerns in the Nation."

So I think there was a broad-based understanding at a time when these computer systems were coming into place and making it possible to create these profiles on Americans that the Social Security numbers' use should be regulated.

But, of course, over the last 30 years, what we have seen instead has been the expanded use of the Social Security number, both by the Federal agencies and in the private sector. So I think it is very appropriate to be looking at legislation today.

I think it is also not surprising, if I might point out, that many of the States all across the country have passed legislation, from New York and West Virginia to Arizona and California and Colorado, limiting the use of the Social Security number in the private sector because so many people have complained in those States about being asked to put their Social Security number on their check or finding their Social Security number on their employee identification card. There is a real push today in the country at the State level to improve safeguards for the use of the Social Security number to try to protect privacy.

Now, I think the two bills under consideration, H.R. 1078 and H.R. 1745, would certainly help. I think a lot of effort has obviously gone into these proposals, and I hope they will be acted upon by the committee. But as you see in my statement, I am actually urging you to consider going somewhat further.

I am concerned, for example, that if too many statutory exceptions are created, if too many of the current business practices that make use of the Social Security number are left in place, we really won't do a particularly good job in safeguarding the privacy of American consumers. And so my hope is that Congress will be able to send a clear message that there may be some circumstances in the private sector where the Social Security number is necessary. It is certainly being used as the tax identification number, and employers need it. And it may also be necessary for fraud investigation, but I think what we need to do today is to limit the use of the Social Security number in the private sector and make clear that there are certain uses, such as the commercial sale of a Social Security number, for which there really is no basis. And I thank you again for the opportunity to be here today.

MR. STEARNS. And I thank you, MR. ROTENBERG.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC
PRIVACY INFORMATION CENTER

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for the opportunity to testify today on Social Security Numbers in commerce and how best to reconcile beneficial uses with threats to privacy.

My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C.¹ Founded in 1994. EPIC has participated in leading cases involving the privacy of the Social Security Number (SSN) and has frequently testified in Congress about the need to establish privacy safeguards for the Social Security Number.² Last year, we

¹ EPIC maintains an archive of information about the SSN online at <http://www.epic.org/privacy/ssn/>.

² See, e.g., *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) (“Since the passage of the Privacy Act, an individual’s concern over his SSN’s confidentiality and misuse has become significantly more compelling”); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) (“the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs”); Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, at a Joint Hearing on Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security (Nov. 8, 2001) available at http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC, at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims (Sept. 19, 2002) available at <http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html>.

testified on H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act of 2005, and urged Members to reject the use of the SSN as a national identifier and to ensure the development of adequate privacy and security safeguard to address the growing crisis of identity theft.³

Social Security numbers have become a classic example of "mission creep." A number that was created for a specific, limited purpose has been transformed for additional, unintended purposes, sometimes with disastrous results. The pervasiveness of the SSN threatens privacy and the financial security of Americans. For example, SSNs are routinely used to both identify and authenticate an individual, a deeply flawed security practice.

SSNs are also used to build detailed profiles on American consumers, linking together records that might otherwise be difficult to match. Without the SSN, businesses would have to be more forthcoming with individuals about the sources of information that are obtained and the profiles that are created. However, the SSN makes it possible to create profiles that are not only detailed but also secretive. As a consequence, consumers are able to exercise less control over their personal information held by others. Absent an explicit statutory protection, they have no idea what information about them is collected, how it is used, or to whom it is disclosed.

The privacy risks associated with the creation of the SSN have been well understood for a long time. Although Congress successfully limited some uses of the SSN by federal agencies with the passage of the Privacy Act in 1974, since that time Congress has largely failed to establish the necessary safeguards to protect American consumers.

History of SSN Use

The Social Security Number (SSN) was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers' contributions to the social security fund. Legislators and the public were immediately distrustful of such a tracking system, which can be used to index a vast amount of personal information and track the behavior of citizens. Public concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security Number that show a striking resemblance to the problems we face today. Although the term "identity theft" was not yet in use, *Records, Computer, and the Rights of Citizens*, the report that provided the basis for comprehensive privacy legislation in 1974, described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."⁴

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of the widespread use of SSNs as universal identifiers, and enacted provisions to limit uses

³ Testimony of Marc Rotenberg, President, Electronic Privacy Information Center, at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005" before the House Judiciary Committee Subcommittee on Immigration, Border Security, and Claims (May 12, 2005) available at <http://www.epic.org/privacy/ssn/51205.pdf>.

⁴ "Records, Computers, and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare 125-35 (MIT 1973).

of the SSN. The Senate Committee report stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." Short of prohibiting the use of the SSN outright, Section 7 of the Privacy Act provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." This provision attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed that the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

However, the Privacy Act failed to limit the use of the SSN by the private sector as the 1973 report had urged. Credit reporting agencies, marketing firms, and more recently, data brokers to build detailed profiles on American citizens exploited this loophole. As a consequence, consumers have experienced the extraordinary problem of identity theft.

Identity Theft

Commercial enterprises have made the SSN synonymous with an individual's identity. Despite the fact that the SSN was never intended to be used for identification purposes, they are considered the "keys to the kingdom" for records about individual consumers.

The financial services sector, for instance, has created a system of files containing personal and financial information on nearly ninety percent of the American adult population, keyed to individuals' SSNs. This information is sold and traded freely, with virtually no legal limitations. This widespread use, combined with lax verification procedures and aggressive credit marketing has led to widespread identity theft.

Credit grantors rely upon the SSN to authenticate a credit applicant's identity; many cases of identity theft occur when thieves apply using a stolen SSN and their own name. Despite the fact that the names, addresses, or telephone numbers of the thief and victim do not match, accounts are opened and credit granted using only the SSN as a means of authentication. EPIC has detailed many of these cases in other testimony.⁵

The root of this problem is that the SSN is used not only to tell the credit issuer who the applicant is, but also to verify the applicant's identity. This would be like using the exact same series of characters as both the username and password on an email account. The fact that this practice provides little security should not be a surprise.

The printing of SSNs on government-issued drivers licenses provided yet another opening for identity thieves. A thief who stole your wallet could also easily steal your identity, with name, address, driver's license number, and SSN in one easy place. Congress recognized this threat and in the Intelligence Reform and Terrorism Prevention Act of 2004, prevented the printing of SSNs on drivers' licenses and other government-issued ID.⁶

States are Taking the Lead on SSN Privacy

Several states have, in recent years, established new privacy protections for SSNs. These laws demonstrate that major government and private sector entities can still operate in environments where disclosure and use of the SSN is limited. They also

⁵ See, e.g., *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (Credit reporting agencies issued credit reports to identity thief based on SSN match despite address, birth date, and name discrepancies); *Dimezza v. First USA Bank, Inc.*, 103 F. Supp.2d 1296 (D. N.M. 2000) (same). See also *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003) (Credit issued based solely on SSN and name, despite clear location discrepancies); *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997) (same); *Vazquez-Garcia v. Trans Union De P.R., Inc.*, 222 F. Supp.2d 150 (D. P.R. 2002) (same).

⁶ Pub. L. No. 108-408 §§7211-7214, 118 Stat. 3638, 3825-3832 (2004).

provide examples of protections that should be considered at the federal level. For example, Colorado, Arizona, and California all have laws that broadly restrict the disclosure and use of the SSN by both government and private actors. These laws encourage agencies and businesses to use different identifiers for their specific purposes, reducing the vulnerability that the disclosure of any one identifier may create.⁷ Arizona's law also prohibits the printing of the SSN on material mailed to Arizona residents, reducing the threat of fraud from intercepted correspondence.

Other states, including New York and West Virginia, have statutes that limit the use of the SSN as a student ID number.⁸ This reduces the vulnerability of students to identity theft and protecting the privacy of students whose personal information is collected in databases, and whose grades are often publicly posted, indexed by their student ID numbers. Similar laws exist in Arizona, Rhode Island, Wisconsin, and Kentucky.⁹

Of course, we would welcome strong legislation in Congress that would limit the use of the Social Security Number in the private sector and help safeguard the privacy interests of American consumers, but the bills now pending before the Committee have been so watered down it is not clear that they would provide much actual benefit. Many exceptions have been created to permit business to continue to collect and use the SSN for a wide range of commercial activities. There are also problems with the lack of effective enforcement. And the bills generally provide less protection than comparable state measures.

Possible SSN Privacy Legislation

I would like today to propose a simple approach to safeguarding privacy and limiting the misuse of the Social Security Number and that is to recommend legislation that would prohibit the collection and use of the Social Security Number by a commercial organization where there is no legal authority to do so. Simply stated, if Congress determined that it was necessary to authorize the use of the SSN in the private sector, as it did when it chose to make the SSN the Tax Identification Number, then a commercial firm would have the legal authority to collect and use the SSN consistent with that statutory purpose. But where there is no legal authority to collect an individual's SSN, the commercial firm would be prohibited from doing so. This would change the default on the use of the SSN and help ensure that the number was used only for appropriate purposes.

You could also, if you wish, apply the approach set out in section 7 of the Privacy Act by requiring private sector organizations that seek to collect an individual's SSN to inform that individual whether the disclosure of the SSN is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of the individual's SSN. Many privacy notices have become extraordinary complex and are routinely ignored. But the original notice for the collection and use of the SSN set out in the Privacy Act of 1974 would actually be very helpful for consumers who are trying to safeguard their privacy.

Either approach would provide meaningful limitations on the use of the SSN, reduce the risk of identity theft, and help restore consumer privacy. These are also the approaches consistent with the Privacy Act of 1974 and the 1973 report that provided the basis for that landmark law.

⁷ Colo. Rev. Stat § 24-72.3-102; Ariz. Rev. Stat. § 44-1373; Cal. Civ. Code § 1798.85.

⁸ N.Y. Educ. Law § 2-b; W. Va. Code Ann. § 18-2-5f.

⁹ Ariz. Rev. Stat. § 15-1823; R.I. Gen. Laws § 16-38-5.1; Wis. Stat. Ann. § 36.11(35); Ky. Rev. Stat. Ann. § 156.160.

Conclusion

The expanded use of the Social Security Number is fueling the increase in identity theft in the United States and placing the privacy of American citizens at great risk. The widespread use of the SSN has made it too easy for government agencies, businesses, and even criminals to create detailed profiles of individuals Americans. Congress wisely sought to limit the use of the Social Security Number by federal agencies when it passed the Privacy Act of 1974, and the states have since established additional safeguards. Still it is clear that the problem of the misuse of the Social Security Number is on the rise.

Effective privacy legislation for the SSN in the commercial sector could be based on either requiring businesses to have legal basis to collect and use the SSN or by applying Section 7 of the Privacy Act to commercial entities.

MR. STEARNS. You have been kind enough to come and testify before, and I think we were in Rome together. So let me just start off with you.

The Gramm-Leach-Bliley and the Fair Reporting Credit Act, do you think that these things specifically should be changed?

MR. ROTENBERG. If you are referring to the security standard in the Gramm-Leach-Bliley Act, I don't think it goes far enough to address the specific problems with the Social Security number. I think that was kind of left as an open issue, and it is one of the reasons why it probably would be appropriate to do some legislation around the SSN.

MR. STEARNS. We have a data security bill that we passed out of my subcommittee and the full committee. Do you think that goes to help a little bit?

MR. ROTENBERG. I think it will probably, and I haven't looked at it recently, but my recollection is that that bill didn't specifically address some of the SSN misuse issues. So that piece I think you could still get to.

MR. STEARNS. We are thinking about perhaps having an amendment. And Chairman Barton has talked about having a markup or a bill in our subcommittee, but we are thinking about possibly having an amendment to the data security bill to include something on Social Security. You say it is not part of it and should be part of it, and we agree.

MR. ROTENBERG. I think that would be a good approach.

MR. STEARNS. Ms. Steinfeld, your testimony describes a practice of furnishing data under the FCRA, in which a company furnishes data to an entity that merely clicks a, quote, "I agree" box; that it has a permissible purpose under the FCRA. Is this a violation of the FCRA?

MS. STEINFELD. Well, what I found was an Internet site that was making a lot of public record information available, and, again, public record information, including the Social Security numbers, is currently lawfully available for sale on line. What the Website said is for the Social Security number, we will only give that out if you have a

permissible purpose under the Fair Credit Reporting Act. And then it said, click here to say, yes, I do have that permissible purpose.

So the point I was making in the testimony is that if you do establish a regime like the two bills are contemplating, one important key piece is to make sure that you verify the identity and the authority of the requester of data that they actually meet one of the exceptions that are in the statute. Having people say, "Yes, I am legitimate," under your law is not enough.

MR. STEARNS. How do we identify a person in a remote location, in a computer, with a click? I mean, how do you identify that person?

MS. STEINFELD. I think it is very difficult, and I think it is what a lot of major industry players have been wrestling with. I have been looking a little bit at some of the ChoicePoint plans and the aftermath of some of their problems, and they have some robust credentialing requirements now that they impose before requesters can request sensitive data. And I have been told by another industry leader lately that there are actually site visits to test the authenticity of the requester when the volume and the sensitivity of the data is so great. But I recognize that is not going to work in all cases, and there is an interest in being able to deliver services online in a sufficient way, and I do think we are still wrestling with how to authenticate identity and authority in an online world.

MR. STEARNS. Mr. Lively, we have touched upon it with the Commissioner Leibowitz when he was here earlier. Let us say, for example, just a hypothetical, the President signed the bill that prohibited a business from refusing to do business with a consumer without receipt of a Social Security number. How would that affect your membership?

MR. LIVELY. It would clearly have an impact on service levels because alternative methodologies would have to be sought out and would have to be pursued, and the timely service that the industry is able to provide to its customers would be seriously deteriorated.

MR. STEARNS. And it would be expensive, I guess.

MR. LIVELY. Very expensive.

MR. STEARNS. Well, you heard the Commissioner's testimony, and there are a lot of members who might vote for banning the sale or purchase of Social Security numbers without the person's consent. And even in certain cases, you heard the Chairman talk about his cell phone, you heard the Commissioner talk about this giving of the Social Security number, so a lot of members are sort of thinking, well, Social Security numbers are something we should not allow to be used, and there might be another identifiable thing.

MR. LIVELY. Yes. I totally understand that and appreciate the concern that is being applied to that particular circumstance, but when the terms are being used about purchasing a Social Security number, you

have to be awfully careful not to cause the credit report, which contains a Social Security number, from being classified as the purchase of a Social Security number. These things are so tightly integrated, and the systems have been developed both from the standpoint of fraud control as well as from the standpoint of customer service, and when you have got those objectives--because, after all, these institutions are in business to provide services to consumers. And by definition, services need to be timely, they need to be accurate, they need to be effective, and they need to provide the customer with the service they intended to obtain from that institution. And today we have situations in which the consumer can go to purchase an automobile and drive the automobile away from the dealership the same afternoon because of the facility--

MR. STEARNS. Quite incredible.

MR. LIVELY. --access to this technology that is driving the Nation's economy. And at the end of the day, the care that has to be taken by this committee and all of the other people who are going to be involved in this process must be very, very, very carefully driven because inadvertent mistakes in the legislative process can create some havoc in the marketplace.

MR. STEARNS. Mr. Ireland, I will close with you and Ms. McDonald. Mr. Ireland, do you see any problems with banning the sale of Social Security numbers to nonfinancial entities? And what nonfinancial entities should have access or require Social Security numbers?

MR. IRELAND. When you talk about the sale of Social Security numbers, if you just mean somebody that is going to offer a list of Social Security numbers for sale, I don't know of a legitimate business purpose for that, and I am not troubled by the idea of banning it to nonfinancial entities. If we are talking about selling a loan file, for example, that includes a Social Security number and that is banned, I have just shut down the secondary mortgage market, among other things.

So I think you have to define your terms carefully, and there are clearly practices out there that you could identify that don't have a legitimate commercial purpose, and you could further restrain, we think, in the case of financial institutions that are already probably prohibited by the Gramm-Leach-Bliley Act. But for nonfinancial institutions, they don't have comparable restrictions. There may be areas where it is appropriate to have further restrictions, but you have to be careful as you do that because Social Security numbers, as part of a loan file or as a component of a larger financial transaction, are sold all the time and are key to many commercial transactions and retail transactions in this country.

MR. STEARNS. Mr. McDonald, perhaps you could, just for illustrative purposes, give us an example, worst practices you may have seen with regard to securing Social Security numbers in your area, if you have any.

MS. MCDONALD. Well, when you say worst practices --

MR. STEARNS. Do you have the speaker on?

MS. MCDONALD. Yes. I am not sure when you are saying worst practices, the abuses we have seen.

From our standpoint, what we see with concerned participants has made them extremely paranoid, and in our service we are doing a good thing. We are finding them, reuniting them, they are excited to, in many cases to be back with their benefits. In other cases, they are calling their congressman and saying, "I got this letter, I don't understand." For our purposes though, if we were not able to get access to Social Security numbers, there's no way we could find a lot of the female participants by a name that is no longer theirs, due to marriage or divorce.

MR. STEARNS. So a Social Security number is the only way you can identify these people, is what you are saying?

MS. MCDONALD. To find the right person, yes. I mean, even in our database with all the people we have located, if somebody gives a name, it takes us forever to go through and give them all the names of the companies that they worked for.

MR. STEARNS. Mr. Rothberg, do you agree with that?

MR. ROTENBERG. I am sorry. The SSN can be useful in locating individuals?

MR. STEARNS. Yes. Social Security number's the only way that you can identify people, and that is why she feels it is so important.

MR. ROTENBERG. Well, I am sure there are circumstances where that may be the case, but I think it is also true that many businesses create their own unique identification numbers. I was thinking about this the other day--

MR. STEARNS. Like the military.

MR. ROTENBERG. Well, the military does, your credit card company, your utility company. I think we are quite used to seeing a lot of different types of identifiers. What is really different about the Social Security number and the reason that it creates both benefits and risks is that it makes it possible to link data across different worlds, financial records and medical records.

MR. STEARNS. My time has expired. The gentleman from Massachusetts.

MR. MARKEY. Thank you, Mr. Chairman, very much. Just to restate a thank you, Mr. Chairman, and the full committee Chairman, Mr. Barton, for having this hearing.

My bill would halt unregulated commerce in Social Security numbers. It does not establish an absolute prohibition on all commercial use of the number, but it would make it a crime for a person to sell or purchase Social Security numbers in violation of rules promulgated by the Federal Trade Commission. The Federal Trade Commission would be given the power to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill's restrictions.

So you actually put together an all-star cast here, a privacy all-star team, both sides represented, I might say, on the issue. Mr. Ireland, if I may begin with you, and welcome back. I remember you with the Fed.

MR. IRELAND. Yes.

MR. MARKEY. Always a vigorous opponent of strong privacy protections, and you are consistent here in your testimony today. And you argue in your testimony that the financial services industry should be exempt from any Social Security number legislation, and in part, because of the existence of the privacy provisions of the Gramm-Leach-Bliley Act. Now, as Debbie Shannon remembers back in 1999 and 2000, sitting right behind you, the financial services industry was actually able to convince the Banking Committee in the House and in the Senate to have no privacy protections in Gramm-Leach-Bliley until it came to this committee when, in a surprise vote, Mr. Bliley sided with me. And pretty much all the privacy in the Gramm-Leach-Bliley is because of the vote in this committee on my amendment.

And as a result, I am very aware of all of the loopholes in that law. As it finally went back over to the Banking Committee conferees as well, successfully worked upon by the financial services industry. So my first question to you, why should your member banks, brokerages, insurance companies be able to sell my Social Security number without my permission?

MR. IRELAND. Well, as I said in a response to Chairman Stearns a little while ago, we don't sell lists of Social Security numbers, and we have no interest in doing that. There are circumstances, however, when you sell loans or groups of loans, and the loan files include Social Security numbers, it is necessary to the secondary mortgage market, for example, to be able to do that.

So to be able to sell Social Security numbers in that context, I think is critical to the effect of operation of the mortgage market and for consumers to be able to enjoy low mortgage rates.

MR. MARKEY. Do you think it would be unrealistic to ask the secondary mortgage market to develop their own individual identifiers for their own clients that would not require them to use Social Security numbers as a universal identifier? How hard can that be?

MR. IRELAND. I think that is actually very, very difficult because one of the things you want to do if you are looking at a mortgage loan in the secondary market is you want to get an assessment of the credit quality of the borrower. So you are not only going to have to be able to identify them as that mortgage loan borrower, but you may want to get a credit report on them to know whether this is a subprime 620 borrower or it is a superprime 820 borrower, that will go into how much you are going to pay for that particular mortgage.

MR. MARKEY. So when companies secure ties, for example, credit card loans, do they always use a Social Security number, or do they have another identifier system which they use?

MR. IRELAND. Well, various companies will attach when they create loans, mortgage loan identifiers.

MR. MARKEY. A different number from the Social Security number.

MR. IRELAND. In addition to the Social Security number.

MR. MARKEY. How can they figure out to do that, but they couldn't-

MR. IRELAND. It is perfectly possible for financial institutions. As a matter of fact, most financial institutions do it all the time to establish unique account numbers for their customers.

MR. MARKEY. So it is possible, is that what you are saying?

MR. IRELAND. And that works very well for identifying people within that financial institution. The problem comes in linking up their identification system with other identification systems. If you are going to transfer assets or you are going to do business across institutions, which is key, as I pointed out, in the example in the secondary mortgage market, but there are numerous other examples.

MR. MARKEY. Yeah. Well, I just kind of disagree with you on that, sir. I just think that we have got an information system now that is so massive in its delivery capacity that it can practically deliver breakfast to you through that wire. And I don't know why we couldn't figure out or these industries couldn't figure out some identifier system that just didn't have to use the Social Security number.

Let me just move on here. Under Gramm-Leach-Bliley, a financial services company doesn't have to get my permission to transfer my personal information, including my Social Security number, to any of its affiliates. If I open a checking account with CitiBank, why should Smith Barney, Diners Club, Primerica, Citi Insurance and the rest of Citigroup's affiliates be able to get a copy of my personal information, including my Social Security number?

MR. IRELAND. Well, as you may recall, one of the principle advantages of the Gramm-Leach-Bliley Act in tearing down the walls between banking and insurance and securities business was to allow the

cross-marketing of those services within financial holding companies. And typically the way that is done, and to be done most cost effectively so the customers enjoy the best price, is out of a common customer database, which identifies customers the same way across the holding company. So the customers can deliver one-stop shopping to their--

MR. MARKEY. All right. So that is one-stop shopping. Let us move to the next stage where they can deliver my Social Security number to any third party with whom the bank has a joint marketing agreement. Does that get into cost effectiveness too?

MR. IRELAND. Well, one of the reasons, as I recall, for the joint marketing agreement exception was to allow smaller banking companies and securities companies to enter into agreements and try to deliver the same kind of one-stop shopping that larger financial services, holding companies do deliver. It was a competitive issue for smaller institutions.

MR. MARKEY. I appreciate it. But why shouldn't they have to get my permission? It is my identity. Why shouldn't they have to come back to me and get my permission?

MR. IRELAND. Well, as you will recall, Gramm-Leach-Bliley basically does an opt-out system for nonaffiliated third parties. If for competitive reasons you wanted to decide that you were going to disadvantage the smaller institutions and provide a greater competitive advantage for larger institutions, I think that has financial structure implications, and my recollection is, that is the rationale for the joint marketing exception. You could disagree with that exception on that basis, but I think that was the rationale.

MR. MARKEY. Yeah. But again, and this goes back to that period of time, I still don't believe that I should have to sacrifice my privacy and give up my Social Security number so that companies can market to me. If I want to give up my privacy, I should be asked to give it up. And that is still a debate, but that gets to the core of the Social Security issue here.

People view that as their identity. And I just don't think that they should be viewed to just even in a way if they open up an account in any part of Citigroup, and now it is just sloshing through the entire Citigroup empire and all third-party relationships that they have. It just gets dangerous in terms of Amy Boyer, murder victim in New Hampshire. Okay, that is how this stuff just sloshes through and out, okay.

Let me ask Mr. Rotenberg and Ms. Steinfeld, do you believe the financial services industry should be exempted from any bill that this committee is crafting to create Social Security number protections of general applicability for all companies in America?

MR. ROTENBERG. Congressman Markey, quite the opposite. I think the financial services industries should be subject to the greatest regulation because they are typically the ones who make the greatest

demand for the Social Security number. Now, there may be some purposes that are appropriate and necessary, as I suggested in my statement, but it is precisely because that industry is making such wide spread use of the SSN that I think we need legal protections.

MR. MARKEY. Okay. Ms. Steinfeld?

MS. STEINFELD. I believe the bill takes the approach of identifying the purpose that you would use the SSN for as the basis for the exception, and I continue to believe that that is the best approach rather than determining that a specific industry should be exempt. In my view, it is better to say, what is the reason for the exemption?

It could very well be that at the end of a rule making, which I believe is the way to go, that many of the purposes that financial services put forward would be considered to be valid purposes, in which case they would get exemptions for those purposes. But again, I think the useful exercise is to really explore what are the legitimate uses, what are the legitimate purposes and that a rule making is a good place to tee those issues up.

MR. MARKEY. Thank you. Now, Mr. Rotenberg, you have suggested that companies should only be able to use and collect Social Security numbers when they have explicit legal authority to do so.

Under current law, what are the circumstances in which there is such a legal authorization for the use of Social Security numbers by the private sector?

MR. ROTENBERG. Well, Congressman, right now we really don't have an approach that sets up legal authority for collecting the SSN. In some circumstances employers, for example, are required to obtain the SSN because it operates also as the employment identification--I am sorry, the tax identification number, and therefore is necessary for various tax filings.

But the point I was trying to make in my statement is I think Congress very wisely, back in the Privacy Act in 1974, was trying to limit the use, and your bill would certainly do this, but the core principle really is you don't ask for the SSN unless you have legal authority to get it.

MR. MARKEY. So are there other circumstances where it would be permissible for a company to be able to collect or buy or sell a citizen's Social Security number?

MR. ROTENBERG. Well, there's some case law that suggests that there could be limitations on the sale of the Social Security number. There was an interesting case a couple of years ago in Washington State, and I have been involved in some litigation surrounding the publication of the SSN, but for the most part, we really don't have any restrictions,

and I think that is what has contributed in part to the growing identity theft.

MR. MARKEY. Thank you. Let me ask, Mr. Ireland, if Congress were to exempt the financial services industry from Social Security number protection legislation, what would prevent Citicorp from acquiring an information broker or creating an in-house information broker that would then not be subject to any rules crafted by the Federal Trade Commission for all other businesses?

MR. IRELAND. Well, if Citigroup acquired an information broker, that broker would, by definition, be a financial institution subject to the Gramm-Leach-Bliley rules, which would also restrict the use of Social Security numbers. I mean, I understand--

MR. MARKEY. But they have all the exceptions, which we just discussed.

MR. IRELAND. They would have all of the exceptions we just discussed.

MR. MARKEY. Right. So Mr. Rotenberg, Ms. Steinfeld, what do you think? What would happen in that kind of a situation where this information broker is now lodged safely inside of Citigroup? What is the status for protection of Social Security numbers?

MS. STEINFELD. I think the status of the Social Security numbers would be pretty legally available for the sharing except if the safeguards rule and the analysis done by Citigroup about security risks and mitigating risks resulted in some curbs on the use of the Social Security numbers.

MR. MARKEY. What if it is not a customer, though? What if it is someone else that wants to buy somebody else's name?

MS. STEINFELD. I am not sure I understand the question. If an outsider wanted to buy information from Citigroup. Well, Mr. Ireland may want to comment.

MR. IRELAND. If I may, first of all, the Citigroup affiliate would be subject to the Federal Reserve Board's rules, not the FTC safeguard's rule, Federal Reserve's security rules for the holding company. And you are correct that those rules do not apply to information about noncustomers except they would have a reuse limitation under the Gramm-Leach-Bliley Act to the extent that they got that information from another financial institution.

One of the things that the data security bill that this committee passed and data security bills that other committees have passed did would be to close that loophole in requiring data security regardless of whether or not it is your customer. And to my knowledge, the financial services industry doesn't have a problem with closing that loophole.

MR. MARKEY. If I may, Mr. Chairman, I would just like to ask each of the witnesses to give us the one-minute nutshell summary of what you want us to remember from your testimony. What do you want us to know about Social Security numbers and what Congress should do about it? We will begin with you, Ms. McDonald. One minute.

MR. STEARNS. Or one sentence.

MS. MCDONALD. Well, what I would like to say is there are beneficial uses to getting access to Social Security numbers. And in the case of a missing participant or incorrect data, I don't know how you would get their approval up front in order to get that information.

MR. MARKEY. Okay. Mr. Lively.

MR. LIVELY. I believe that one of the most important things that I would like to leave with you folks is the fact that we are very concerned about unintended consequences of a legislative process that hasn't gone deep enough to make sure that there is not going to be a very downside impact of the changes that are made in the law.

MR. MARKEY. Ms. Steinfeld.

MS. STEINFELD. I would say that it is surprising to me that data as sensitive as the Social Security number is so unregulated, and so I do think it is appropriate to ban the uncontrolled sale and purchase of Social Security numbers. But this has to be done with extreme care for the reasons that all the panelists have described. And a rule making with such attention to public comment and agency expertise and the FTC is an appropriate way to go.

MR. MARKEY. Mr. Ireland.

MR. IRELAND. I would echo Mr. Lively's comment that any requirement should be made with a full understanding of how they affect current legitimate business transactions so that we try to avoid unintended consequences.

MR. MARKEY. And Mr. Rotenberg.

MR. ROTENBERG. Congressman, I think the Social Security number has been pretty much a ticking privacy bomb from the time it was created, and I think the SSA has known this. I think Congress has known this. And I think the American public knows it. And I think in the end, we are going to need some legislation to ensure that the privacy risks associated with the misuse of the SSN are minimized.

MR. MARKEY. Thank you all very much. Mr. Chairman, I can't thank you enough for your patience.

MR. STEARNS. Well, thank you for coming back. And I want to thank the panel for their patience while we had all the votes in the House floor.

I think that for a lot of members, we are just so surprised that there is no penalty, civil or criminal, for the sale of Social Security numbers, and

we have sort of let this thing go. So it is time we do something. So I am encouraged that Chairman Barton has said we are going to try to have a markup or have a bill.

And so I think your patience here has helped a lot of us understand it better. We have a written record now that we will use when we go back to debate and to convince our colleagues of the importance.

So with that, the subcommittee's adjourned.

MR. LIVELY. Mr. Chairman would it be appropriate to submit my entire testimony, my written testimony?

MR. STEARNS. By unanimous consent, so ordered.

MR. LIVELY. Thank you, sir.

[Whereupon, at 5:50 p.m., the subcommittee was adjourned.]

