PROTECTING THE PRIVACY OF CONSUMERS' SOCIAL SECURITY NUMBERS

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 28, 2004

Serial No. 108–128

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

96-100PDF WASHINGTON : 2004

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*

W.J. "BILLY" TAUZIN, Louisiana
RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
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
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
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma

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
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JANICE D. SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas

BUD ALBRIGHT, *Staff Director*
JAMES D. BARNETTE, *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
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
Vice Chairman
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma
JOE BARTON, Texas,
(Ex Officio)

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
CHARLES A. GONZALEZ, Texas
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

PROTECTING THE PRIVACY OF CONSUMERS' SOCIAL SECURITY NUMBERS

TUESDAY, SEPTEMBER 28, 2004

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 p.m., in room 2123, Rayburn House Office Building, Hon Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Barton (ex officio), Schakowsky, and Green.

Also present: Representative Shaw.

Staff present: David Cavicke, majority counsel; Chris Leahy, policy coordinator; Shannon Jacquot, majority counsel; Brian McCullough, majority professional staff member; William Harvard, legislative clerk; and Ashley Groesbeck, minority research assistant.

Mr. STEARNS. The subcommittee will come to order.

Good afternoon. I am pleased to hold this important hearing on H.R. 2971, the Social Security Privacy Identity Theft Prevention Act of 2003. The committee received a referral on the bill, and this subcommittee will take a good look at the issues which surround this legislation.

My colleague from Florida, Congressman Shaw, has done a great deal of work on this bill and in this area. I commend him for his work as an 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. Now, my colleagues, identity theft is a very important consumer protection issue. Federal Trade Commission data indicates in a 1-year period, from September 2002 to September 2003, over 10 million people were victims of identity theft. That also means 297 million hours were spent in the year 2003 cleaning up the identity theft problem. So people talk about the numbers in terms of people and money spent, but the hours are also a great deal.

I also point out that the loss to businesses were $48 billion in 2003 and $5 billion in 2003 to individuals. So, frankly, this is a significant cost to consumers and businesses both in terms of money lost and time spent trying to clear up their names and, obviously, correct their 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 have to make as legislators. 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 itself has for reducing the occurrence of this problem.

This committee has extensive knowledge on issues relating to information privacy and information security. In fact, ladies and gentlemen, this will be my eighth privacy hearing on this subcommittee in the past 3 years dealing with privacy and information security. I have a privacy bill, which I introduced in the 170th Congress and which the committee has had extensive dialog on, providing privacy and security protection for Social Security numbers and other personal identifiable information. So I will continue to work on this problem in this Congress and, God willing, the next Congress.

The anti-spyware bill that was reported by the full committee in July also came through this subcommittee, provides for strong enforcement against spyware practices that, frankly, facilitate identity theft. Phishing and keystroke logging are explicitly prohibited in the bill, and the bill provides that the Federal Trade Commission will have strong enforcement tools to go after these practices. We expect this spyware to be voted in the House this week, hopefully, on the floor under suspension.

So our subcommittee and Congresswoman Mary Bono, who authored the bill and went through our committee, and the great staff we have have made this possible. So we are hoping it will be on the floor this week.

I know the chairman of the full committee, Joe Barton, has intense interest in information and privacy; and I expect this committee will continue to work on it in the 109th Congress.

The heart of this committee's jurisdiction over H.R. 2971 obviously is the Federal Trade Commission and its enforcement practices, and that is going to be a piece of this legislation. That provision makes it an unfair and deceptive act or practice under the Federal Trade Commission for any person to refuse to do business with an individual because the individual will not consent to that person's receipt of his personal Social Security number. The section provides an exception for any case in which a business is required by law to submit to the Federal Government the consumer's Social Security number.

I ask our panel whether there are any other uses of Social Security numbers that are outlawed by this provision but, given appropriate safeguards, would benefit to consumers. That perhaps is one thing you will need to address. I would like to know from this panel what types of information security practice should be implemented when Social Security numbers are exchanged. So I look forward to a frank discussion on this bill at this hearing.

We have a distinguished panel of experts to educate us about this identity theft, privacy in general and importance of the integrity of Social Security numbers. I thank the witness from the Federal Trade Commission, and I thank GAO and EPIC for their participation today.

With that, I welcome the opening statement of the ranking member, the gentlelady, Ms. Schakowsky.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns, and thank you for holding today's hearing on H.R. 2971, the Social Security Number Privacy and Identity Theft Protection Act. This bill, which would restrict what both the public and private sectors can do with Social Security numbers, is an important tool in the fight against identity theft.

Identity theft, as you mentioned, Mr. Chairman, is one of the fastest-growing financial crimes in the United States, with the number of victims doubling each year over the past 3 years. As the Federal Trade Commission reports, in 2003, there were nearly 10 million Americans victimized by this crime. Over the past 5 years, there have been 27 million victims. Both of our States, Chairman Stearns, rank in the top ten for identity theft occurrences. Florida is fifth, and Illinois is ninth.

Although nearly half of the victims do not know how their personal information was stolen, we do know that Social Security numbers are one of the most important means that identity thieves use to financially establish themselves as someone else. When we consider what the financial door of Social Security numbers can unlock and the pervasiveness of the use of these numbers, then the rising number of occurrences of identity theft should come as no surprise.

As we have all personally experienced, everyone wants our Social Security number. It is not just when we open a bank account or apply for a credit card or even when we accept a new job. Our Social Security number is requested when we get an insurance policy, open a new phone account, or sign a lease.

So many times when we establish a business relationship, the other party wants our number, whether there is a legitimate need for it or not. Most times, consumers provide it. We feel we have to do so. But we are so used to being asked for our Social Security number that we may not give enough thought to what the other party might do with it. That company may sell them. The numbers may be transmitted over the Internet for legitimate purposes but may not be protected in those transmissions. Our new accounts may be linked to our Social Security numbers. The numbers may be displayed on forms or files that are not adequately protected.

These possibilities should give everyone pause. If we can limit how other parties, public and private, 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. It can take years to discover that one has been victimized or even longer to repair that damage. That is why I am very pleased we are considering H.R. 2971 today.

Again, it is truly an important start. However, I also believe that we can and need to do more. We, as government officials, need to make sure there are adequate resources for consumers both to prevent them from becoming victims and to help them if they are victimized. We need to make sure we are also helping consumers protect themselves by giving them the information they need to do so. We need to make sure everyone knows how to check their credit

reports regularly. That is how most people find out that they were victimized. We need to make sure that there is help available for victims to recover their losses and to clean up their credit reports with as little hassle and frustration as possible. We need to be as proactive and responsive as we can.

I look forward to continuing the conversation about what we need to do; and, although we have a small panel of witnesses before our subcommittee, I am pleased you could join us today. I look forward to hearing from you.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. GEORGE RADANOVICH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, I would like to thank you for holding this important hearing today on the privacy of consumers' social security numbers.

The social security number was created to identify each U.S. citizen for the sole purpose of tracking employment and benefits however, over time our social security number has been used by both public and private entities for purposes both related and unrelated to the social security program. The usage of this unique identifier has benefited both businesses and consumers, but unfortunately it has led to misuse and most importantly identity theft.

The FTC has reported that over 10 million people were victims of identity theft in one year and they estimate that this translates into upwards of a $48 billion loss for businesses and $5 billion loss for consumers, but a price tag can not be put on the loss of one's identity.

I look forward to hearing our witness' testimony today. Hopefully this will help us determine if our current laws are adequate enough to protect the integrity of our social security numbers and if not, what we need to do to protect them.

PREPARED STATEMENT OF HON. JOHN SULLIVAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OKLAHOMA

Thank you, Mr. Chairman, for holding this hearing.

This is an important issue for the First district of Oklahoma. Oklahomans have a firm appreciation for, and dedication to, the concept of individual liberty. While we conform to our nation's laws, we demand that the federal government respects our liberties and privacy. And this includes first and foremost, our social security number.

The social security number (SSN) was first introduced as a device for keeping account of contributions to the Social Security system. Through the years, however, the government and the private sector have expanded the use of this identifying number. In the view of some, including many of my constituents, a person's SSN has essentially attained the status of a national identification number. SSN's can be required to obtain a driver's license, apply for public assistance, donate blood, take out a loan, access insurance records, track down student loan defaulters, or compile direct marketing mailing lists. Private sector use of the social security number is widespread, and continues to be unregulated by the federal government. This is unacceptable.

H.R. 2971, Social Security Number Privacy and Identity Theft Prevention Act of 2003, prohibits Federal, State, and local governments from requiring the display of SSNs to the general public, displaying SSNs on checks, driver's licenses, and motor vehicle registrations. It would prohibit from employing prisoners in jobs that provide them with access to SSNs. Requiring the transmission of SSNs over the Internet without encryption or other security measures would also become illegal.

Additionally, the private sector could not sell, purchase, or display a SSN to the general public. Businesses would be discouraged from denying services to individuals who refuse to provide their SSNs, unless required by law, by subjecting them to penalties under Federal law. It would create new criminal and civil penalties for violations of this law.

I strongly support H.R. 2971 and the spirit of liberty it upholds. The people of my district, and of all of Oklahoma, commend the gentleman Mr. Shaw for his hard work on this bill. I encourage all members of this Committee to look at this issue very closely, and to support this legislation in order to protect your constituent's privacy.

Thank you, Mr. Chairman.

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

Thank you Mr. Chairman for holding this hearing on H.R. 2971, the Social Security Privacy and Identity Theft Prevention Act of 2003. The Committee received a referral on the bill and we intend to give this issue a fair hearing.

Identity theft is a burgeoning problem for consumers and businesses. Approximately 3.23 million consumers were victims of identity theft in 2003. Losses to business were estimated at $48 billion and losses to individuals were estimated at $5 billion. It is estimated that in 2003, identity theft victims spent 297 million hours trying to clear up the problems and their reputation. Unfortunately, the one unique number than can be used to verify an individual can create hazardous results when it is in the hands of the wrong people.

This Committee has a deep bench of experts in the areas of identity theft and privacy. Over the past three years, Chairman Stearns has held numerous hearings parsing through important issues surrounding information privacy. I too have a very strong interest in information privacy.

Representative Shadegg was the author of an important public law, the Identity Theft and Assumption Deterrence Act of 1998. That Act has provided significant tools for enforcement against identity theft. It also directed the Federal Trade Commission to set up an identity theft consumer resource center. That center has been a success as it has gathered important information regarding identity theft, acted as a central repository for complaints, and provided important consumer education.

We have also worked hard at this Committee to shut down new electronic means to identity theft. The anti-spyware bill sponsored by Representatives Bono and Towns provides the Federal Trade Commission with powerful tools against spyware programs, in particular keystroke logging programs, used to steal personally identifiable information, including a social security number. The bill also includes a prohibition against Phishing, the practice of inducing a consumer to provide personally identifiable information by misrepresenting the identity of the person seeking the information.

I look forward to hearing from our witnesses today on this important topic. Thank you and I yield back.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

I'd like to thank Chairman Stearns and Ranking member Schakowsky for their leadership on this issue.

I have been a long time supporter of protecting our citizens from identity theft. In fact, every year we hold a "How to Prevent Identity Theft" workshop for senior citizens in our district. This has become one of our more popular community events with senior citizens.

Today's seniors did not grow up in the digital age and new technologies can often be confusing. This is why I'm glad to be holding this hearing to ensure we protect senior citizens and the rest of us from identity theft. Advances in technology have led to advances in identity theft and many of the seniors in our district feel vulverable.

Our social security numbers are widely used in both the public and private sectors. Our medical histories and credit records are often tied to our social security number. Given this fact, it is important for both the government and the private sector to maintain the highest degree of security surrounding these numbers.

I support limiting the sale of social security numbers to the general public. However, I also support each of our ability to access those numbers when it comes to checking our own records regarding our personal financial histories or medical histories.

I hope we examine the need to strengthen privacy restrictions pertaining to our social security numbers as we move forward with this legislation.

We will hear testimony today that billions of dollars are lost on identity theft each year. Both business and consumers lose out when identity thieves open bogus accounts and spend money that isn't theirs.

We need to make sure it's as difficult as possible for people to take our money and destroy our credit history.

I look forward to hearing what we can do to make our social security numbers more secure and I thank our panel for coming here today to testify.

Thank you and I yield the balace of my time.

Mr. STEARNS. With that, we will move to our panel, if you will come to the table here.

We have the Honorable Thomas Leary, Commissioner of the Federal Trade Commission; and we have Barbara Bovbjerg, Director of Education, Workforce and Income Security, Government Accountability Office; and Chris J. Hoofnagle, Associate Director of Electronic Privacy Information Center. We welcome your opening statement.

Commissioner, we will start with you. Thank you for your time, and the floor is yours.

STATEMENTS OF THOMAS B. LEARY, COMMISSIONER, FEDERAL TRADE COMMISSION; BARBARA D. BOVBJERG, DIRECTOR, EDUCATION, WORKFORCE AND INCOME SECURITY, GOVERNMENT ACCOUNTABILITY OFFICE; AND CHRIS JAY HOOFNAGLE, ASSOCIATE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. LEARY. Again, thank you, Mr. Chairman. It is a pleasure to be here.

My written statement has been submitted for the record, and that reflects the views collectively of the Commission. My oral responses to you are my own.

As you mentioned in your opening statement—and I won't repeat the numbers—identity theft is a significant problem, and our data indicate that it is a problem which is growing. However, we are heartened somewhat by the fact that most of the recent increase seems to involve misuse of existing accounts rather than opening new credit lines, which is an activity that is somewhat less harmful and somewhat easier for consumers to rectify. We also anticipate that the recently enacted Fair and Accurate Credit Transactions Act of 2003, FACTA, will make inroads into the identity theft problem, but it is much too early to see the results.

We have, as you probably know, a complex rulemaking task under that statute. Notice and comment rulemaking is necessarily a somewhat lengthy process, and we are still in the process. I have a chart that shows the progress of our rulemaking thus far. That process is still under way. And of course, once the rules are in place, it takes some time for business to adjust to a new regime.

So it is too early to tell now whether or not that statute will do what it is intended to do. However, the survey results that we have up to now demonstrate the need for a concerted effort between the public and the private sectors to reduce identity theft.

A second point. If we focus specifically on Social Security numbers, we have to recognize that the effects of their disclosure can be beneficial as well as harmful, as you pointed out in your opening statement, Mr. Chairman. There is no question that identity thieves use the Social Security number as the key to access other peoples' financial resources. ID theft will be we reduced to the extent we make it hard for thieves to get these numbers.

On the other hand, Social Security numbers are essential for the operation of our financial system. Instant access to credit, which we all use for both large and small transactions, would be com-

promised if Social Security numbers could not be used to match consumers to their financial information.

We must find, as you pointed out, the proper balance between the need to keep Social Security numbers out of the hands of identity thieves and the need for businesses to have sufficient information to catch fraud and to match financial records with the right person. Achievement of this goal depends not only on Congress and government agencies but on private business initiatives and prudent actions by consumers themselves.

Three, Congress created important new protections in FACTA. Many of the provisions of the Fair and Accurate Credit Transactions Act of 2003 aim to prevent ID theft and facilitate early detection by the victims:

A, free annual file disclosures. The law requires that consumers be given free access to their credit reports annually. This will enhance their ability to discover and correct errors and detect identity theft early.

B, National Fraud Alert System. The National Fraud Alert System created by this statute will put potential creditors on notice that they must proceed with caution when granting credit in a consumer's name.

C, the so-called "red-flag" rulemaking, which will require financial institutions to analyze identity theft patterns.

And, D, the disposal rule. Rules on the disposal of consumer report information and records will help to ensure that sensitive consumer information, including Social Security numbers, is not simply thrown out with the trash.

When fully implemented, these provisions should help to reduce the incidence of identity theft and help victims recover when problems do occur.

Point four, the role of the Federal Trade Commission. The Commission's law enforcement role in this area is limited. We do not have criminal authority; and criminal sanctions, are, of course, the principal deterrent to crimes such as these. Our primary role today is to maintain a central repository of ID theft complaints for the benefit of other law enforcement agencies. We also work with businesses on developing better ways to protect valuable consumer information. We have a kit available on-line which provides guidance for businesses on this subject. The Commission is also required by FACTA to study how credit reporting agencies use identifying information to match consumers to their credit reports before releasing them.

And finally, and perhaps most important, are education and assistance for consumers. We have published booklets with basic information and specific guidelines for actual victims in both English and in Spanish. I have brought some samples of these booklets today. These have been distributed in the millions. I don't have the exact figure, but it is in the millions.

Mr. STEARNS. We will have the staff bring them up so the ranking member and I can look at them.

Mr. LEARY. In this area, as in other areas, the consumers are better informed; and more wary consumers are always the first line of defense.

In conclusion, let me just say there is no magic bullet that will eliminate identity theft. The basic problem is that the dissemination of personal identifiers is essential for maintaining our financial system that runs on credit, but that same information in the wrong hands can cause immense harm. An appropriate balance of public and private efforts will help to contain the problem, and we in the Commission are determined to do our part.

Thank you very much, Mr. Chairman.

[The prepared statement of Thomas B. Leary follows:]

PREPARED STATEMENT OF HON. THOMAS B. LEARY, COMMISSIONER, FEDERAL TRADE COMMISSION

I. INTRODUCTION

Mr. Chairman, and members of the Subcommittee, I am Commissioner Thomas B. Leary 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. The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. Through this testimony, the Commission will describe the results of a recent survey on the prevalence and impact of identity theft, the ways in which Social Security numbers are collected and used, new protections for consumers and identity theft victims, and the Commission's identity theft program.

II. UNDERSTANDING THE IMPACT OF IDENTITY THEFT

On November 1, 1999, the Commission began collecting identity theft complaints from consumers in its national database, the Identity Theft Data Clearinghouse (the "Clearinghouse").[2] Every year since has seen an increase in complaints.[3] The Clearinghouse now contains over 666,000 identity theft complaints taken from victims across the country. By itself, though, these self-reported data do not allow the FTC to draw any firm conclusions about the incidence of identity theft in the general population. To address this important issue, the FTC commissioned a survey last year to gain a better picture of the incidence of identity theft and the impact of the crime on its victims.[4] The results were startling. The data showed that within the 12 months preceding the survey, 3.23 million persons discovered that an identity thief opened new accounts in their names. An additional 6.6 million consumers learned of the misuse of an existing account.[5] Overall, nearly 10 million people—or 4.6 percent of the adult population—discovered that they were victims of some form of identity theft. These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to individual victims, and almost 300 million hours spent by victims trying to resolve their problems.

Moreover, identity theft is a growing crime. The survey indicated a significant increase in the previous 2-3 years—nearly a doubling from one year to the next, although the research showed that this increase has recently slowed. Notably, this re-

---

[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.

[2] *See infra* Section V for a discussion of the Commission's mandate to maintain an identity theft complaint database pursuant to the 1998 Identity Theft Assumption and Deterrence Act.

[3] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

[4] The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at http://www.consumer.gov/idtheft/stats.html.

[5] These 6.6 million victims include 5.1 million victims who experienced only the unauthorized use of their existing credit card accounts, and 1.5 million who reported the misuse of other existing accounts, such as their checking or telecommunications accounts. Of the cases involving only the misuse of existing credit cards, 26% of the victims (which represents 4.6% of all identity theft victims) reported that the suspect was a family member. Some in the financial services industry do not consider unauthorized use of existing credit card accounts "identity theft" unless accompanied by an "account takeover," meaning that the thief has impersonated the victim to the credit card issuer and has taken actions such as changing the victim's billing address, having a replacement or additional credit card sent out, or changing the victim's password. Federal criminal law, however, defines identity theft to include the misuse of existing accounts. 18 U.S.C. § 1028(a)(7). Of the 5.1 million victims reporting only the unauthorized use of an existing credit card account, 16% reported account takeover.

cent increase primarily involved the misuse of an existing account, which tends to cause less economic injury to victims and is generally easier for them to identify and fix. Overall, the 2003 survey analysis puts the incidence rates of identity theft into sharper focus, and demonstrates the need for a concerted effort between the public and private sectors to act aggressively to reduce identity theft.

III. SOCIAL SECURITY NUMBER USES AND IDENTITY THEFT

Social Security numbers play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Preventing identity thieves from obtaining Social Security numbers will help to protect consumers from this pernicious crime. The potential for misuse arises because Social Security numbers are crucial to the proper functioning of our financial system. Social Security numbers are used to match consumers to their credit and other financial information. Without them, information may be attributed to the wrong consumer, and the accuracy of credit reports may be degraded. Enabling Social Security numbers to be used appropriately will help to ensure that consumers continue to enjoy the benefits of our current credit system. The Commission is studying "the efficacy of increasing the number of points of identifying information that a credit reporting agency is required to match to ensure that a consumer is the correct individual to whom a consumer report relates before releasing a consumer report to a user" as required by the Fair and Accurate Credit Transactions Act of 2003.[6] This study, to be completed by December, 2004, should greatly increase our knowledge of the importance of Social Security numbers in the matching process. The Commission looks forward to reporting its findings to Congress.

Social Security numbers are collected by public and private entities for various purposes, and several federal and state laws restrict the use or disclosure of Social Security numbers, depending on the source.[7] The nationwide credit bureaus are primary private sources of Social Security numbers, collecting information from financial institutions for credit reporting purposes. This information typically includes a consumer's identifying information—such as name, address, and Social Security number—as well as information related to the consumer's credit accounts. The identifying information collected by the credit bureaus is one of the most reliable and comprehensive sources of this information, because individuals tend to provide their financial institutions with accurate and up-to-date identifying information and the credit bureau databases contain information for over 200 million consumers.[8]

The Gramm-Leach-Bliley Act ("GLBA")[9] imposes certain restrictions on the reuse and redisclosure of the identifying information—including Social Security numbers—that is collected by credit bureaus from financial institutions.[10] As a general matter, the GLBA prohibits financial institutions from disclosing nonpublic personal information ((NPI() to nonaffiliated third parties without first providing consumers with notice and the opportunity to opt out of such disclosure. This general restriction, however, is subject to certain exceptions. The information may flow from financial institutions to others for certain purposes specified in the statute and rule, including, for example, to process transactions or to report consumer information to

---

[6] Pub. L. No. 108-159, § 318 (2003).

[7] As GAO has reported, government and commercial entities use Social Security numbers for a number of different purposes, including to verify the eligibility of applicants, manage records, and conduct research. U.S. General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: Feb. 16, 1999) and *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002). As examined in GAO's most recent report of January 2004, information resellers, consumer reporting agencies, and health care organizations obtain social security numbers both directly from consumers and other businesses, and the entities use them for various purposes, including identification and to match the consumer to information stored in the consumer's credit report. *See* U.S. General Accounting Office, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs and Laws Limit the Disclosure of This Information*, GAO-04-11 (Washington, D.C.: Jan. 22, 2004).

[8] *See* Consumer Data Industry Association's Web site, *available at* http://www.cdiaonline.org/about.cfm.

[9] 15 U.S.C. § 6801 *et seq.*

[10] The GLBA applies to any "nonpublic personal information" ("NPI") 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 aa name, Social Security number, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.*, 65 Fed. Reg. 33,646, 33680 (May 24, 2000) (the FTC's Privacy Rule). This identifying information generally is not covered by the Fair Credit Reporting Act. *See FTC v. Trans Union*, Dkt. 9255, Op. of the Commission at pp. 30-31 (Mar. 1, 2000) (holding that consumer name, Social Security number, address, telephone number, and mother's maiden name do not constitute a consumer report under the FCRA).

credit bureaus.[11] When information is disclosed under these GLBA exceptions, the recipient may not use or disclose that NPI except (in the ordinary course of business to carry out the activity covered by the exception under which...the information [was received].([12]

IV. NEW PROTECTIONS FOR IDENTITY THEFT VICTIMS

On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted.[13] Many of the provisions amend the Fair Credit Reporting Act ("FCRA"),[14] and provide new and important measures to prevent identity theft and facilitate identity theft victims' recovery. Some of these measures will take effect this year.[15] They will codify many of the voluntary measures initiated by the private sector and improve other recovery procedures already in place.

One prominent benefit of these amendments to the FCRA is the greater access to free consumer reports.[16] Previously under the FCRA, consumers were entitled to a free consumer report only under limited circumstances.[17] Beginning in December of this year with a regional rollout, nationwide and nationwide specialty consumer reporting agencies[18] must provide free credit reports to consumers once annually, upon request.[19] Free reports will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also enable consumers to detect identity theft early.

Other measures that act to prevent identity theft include:

- *National fraud alert system:*[20] Consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home,[21] can place an alert on their credit files. The alert will put potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the "joint fraud alert" initiative administered by the three major credit reporting agencies. After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each credit reporting agency now shares that request with the other two nationwide credit reporting agencies, thereby eliminating the need for the victim to contact each of the three agencies separately.
- *Truncation of credit and debit card receipts:*[22] In some instances, identity theft results from thieves obtaining access to account numbers on credit card receipts. FACTA seeks to reduce this source of fraud by requiring merchants to truncate the full card number on electronic receipts. The use of truncation tech-

---

[11] These exceptions are found in § 502(e) of the GLBA, and in §§313.14 and 313.15 of the FTC's privacy rule. The other GLBA privacy rules contain substantially similar provisions. The § 313.14 exceptions relate to the processing and servicing of transactions at the consumer's request, and the § 313.15 exceptions contain a broad range of unrelated exceptions, such as preventing fraud, assisting law enforcement, complying with subpoenas, and reporting to credit bureaus. Section 313.13 also contains an exception to the notice and opt out requirement, but that section is not relevant here because it relates to contractual arrangements with service providers and joint marketers.

[12] 16 C.F.R. 313.11(a)(1)(iii), (c)(3) (2000).

[13] Pub. L. No. 108-159 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

[14] 15 U.S.C. § 1681 *et seq.*

[15] The statute set effective dates for certain sections and required the Commission and the Federal Reserve Board jointly to set effective dates for the remaining sections. *See* Effective Dates for the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 602.1 (2004).

[16] Pub. L. No. 108-159, § 211 (2003).

[17] Previously, free reports were available only pursuant to the FCRA when the consumer suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was on welfare. Absent one of these exceptions, consumers had to pay a statutory "reasonable charge" for a file disclosure; this fee is set each year by the Commission and is currently $9. *See* 15 U.S.C. § 1681j. In addition, a small number of states required the CRAs to provide free annual reports to consumers at their request.

[18] Section 603(w) of the FCRA defines a "nationwide specialty consumer reporting agency" as a consumer reporting agency that compiles and maintains files on consumers relating to medical records or payments, residential or tenant history, check writing history, employment history, or insurance claims, on a nationwide basis. 15 U.S.C. § 1681a(w).

[19] *See* Free Annual File Disclosures, 16 C.F.R. §§610.1 and 698.1 (2004).

[20] Pub. L. No. 108-159, § 112 (2003).

[21] The Commission is developing a rule on the duration of this active duty alert. *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23372 (April 28, 2004) (to be codified at 16 C.F.R. pt. 613).

[22] Pub. L. No. 108-159, § 113 (2003).

nology is becoming widespread, and some card issuers already require merchants to truncate.[23]

- *"Red flag" indicators of identity theft:*[24] The banking regulators and the FTC will jointly develop a rule to identify and maintain a list of "red flag" indicators of identity theft. The goal of this provision is for financial institutions and creditors to analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.
- *Disposal of Consumer Report Information and Records:*[25] The banking regulators and the FTC are coordinating a rulemaking to require proper disposal of consumer information derived from consumer reports.[26] This requirement will help to ensure that sensitive consumer information, including Social Security numbers, is not simply left in a trash dumpster, for instance, once a business no longer needs the information.[27]

FACTA also includes measures that will assist victims with their recovery. These provisions include:

- *Identity theft account blocking:*[28] This provision requires credit reporting agencies immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits an identity theft report,[29] unless there is reason to believe the report is false. Blocking would mitigate the harm to consumers' credit records that can result from identity theft. Credit reporting agencies must also notify information furnishers who must then cease furnishing the fraudulent information and may not sell, transfer, or place for collection the debt resulting from the identity theft.
- Information available to victims:[30] A creditor or other business must give victims copies of applications and business records relating to the theft of their identity at the victim's request. This information can assist victims in proving that they are, in fact, victims. For example, they may be better able to prove that the signature on the application is not their signature.
- *Prevention of re-reporting fraudulent information:*[31] Consumers can provide identity theft reports directly to creditors or other information furnishers to prevent them from continuing to furnish fraudulent information resulting from identity theft to the credit reporting agencies.

When fully implemented, these provisions should help to reduce the incidence of identity theft, and help victims recover when the problem does occur.

V. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[32] The Identity Theft Act strengthened the criminal laws governing identity theft[33] and focused on consumers as victims.[34] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints, to make available and to refer these complaints to law enforcement for their investigations, and to provide victim assistance and consumer education. Thus, the FTC's

---

[23] FACTA creates a phase-in period to allow for the replacement of existing equipment.

[24] Pub. L. No. 108-159, § 114 (2003).

[25] *Id.* § 216.

[26] Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21388 (April 20, 2004) (to be codified at 16 C.F.R. pt. 682).

[27] In its outreach materials, the FTC also advises consumers to shred any sensitive information before disposing of it.

[28] Pub. L. No. 108-159, § 152 (2003).

[29] The Commission is developing a rule to define the term "identity theft report." *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23371 (April 28, 2004) (to be codified at 16 C.F.R. pt. 603).

[30] Pub. L. No. 108-159, § 151 (2003).

[31] *Id.* § 154.

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

[33] 18 U.S.C. § 1028(a)(7) made identity theft a crime by focusing on the unlawful use of an individual's "means of identification," which broadly includes "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, Social Security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

[34] Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

role under the Act is primarily one of facilitating information sharing among public and private entities.[35]

To fulfill the Act's mandate, the Commission implemented a program that focuses on three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website, (2) maintaining and promoting the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Assisting Identity Theft Victims

The Commission takes complaints from victims through a toll-free hotline, 1-877-ID THEFT (438-4338),[36] and a secure online complaint form on its website, www.consumer.gov/idtheft. In addition, the FTC provides advice on recovery from identity theft. Callers to the hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities.[37] Victims are currently advised to:[38] (1) obtain copies of their credit reports from the three national consumer reporting agencies and have a fraud alert placed on their credit reports;[39] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the FCRA,[40] the Fair Credit Billing Act,[41] the Truth in Lending Act,[42] and the Fair Debt Collection Practices Act.[43] If another federal agency can assist victims because the nature of the victims' identity theft falls within such agency's jurisdiction, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form, which allows victims to enter their identity theft information into the Clearinghouse. Victims also immediately can read and download all of the resources necessary for reclaiming their credit record and good name, including the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*.[44] The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims and how to correct more intensive credit-related problems that may result from identity theft. It also describes other federal and state

---

[35] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Corporate Marketing Solutions, Inc.*, CIV-02 1256 PHX RCB (D. Ariz. Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards); *FTC v. C.J.*, CIV-03 5275 GHK (RZx) (C.D. Cal. July 24, 2003) (final order); *FTC v. Hill*, CV-H-03-5537 (S.D. Tex. Dec. 3, 2003) (final order); and *FTC v. M.M.*, CV-04-2086 (E.D.N.Y. May 18, 2004) (final order) (defendants sent "phishing" spam purporting to come from AOL or Paypal and created look-alike websites to obtain credit card numbers and other financial data from consumers that defendants used for unauthorized online purchases). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (Jan. 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

[36] The Commission has a separate toll-free line (877-FTC-HELP) to serve those with general consumer protection complaints.

[37] Spanish speaking counselors are available for callers who select the Spanish-language option on the toll-free line.

[38] As the relevant provisions of FACTA become effective, the Commission will update its advice to victims on their new rights and procedures for recovery.

[39] These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name.

[40] 15 U.S.C. § 1681 *et seq.*

[41] *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[42] *Id.* § 1601 *et seq.*

[43] *Id.* § 1692 *et seq.*

[44] *Identity Theft: When Bad Things Happen to Your Good Name* and the secure complaint form are available in Spanish.

resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.4 million copies of the booklet since its release in February 2000, and recorded over 1.6 million visits to the Web version.[45]

B. The Identity Theft Data Clearinghouse

One of the primary purposes of the Identity Theft Act was to enable criminal law enforcement agencies to use a single database of victim complaints to support their investigations. To ensure that the database operates as a national clearinghouse for complaints, the FTC accepts complaints from external sources such as other state or federal agencies as well as directly from consumers through its call center and online complaint form. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the prevalence of identity theft complaints by states and by cities.[46] Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse in July of 2000, more than 1042 law enforcement agencies, from the federal to the local level, have signed up for secure online access to the database. Individual investigators within those agencies have the ability to access the system from their desktop computers 24 hours a day, seven days a week.

The Commission actively encourages even greater use of the Clearinghouse. Beginning in 2002, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the United States Postal Inspection Service, and the United States Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, seminars have been held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, Phoenix, New York City, Seattle, San Antonio, Orlando, Raleigh, Rochester, and Denver. The FTC also helped the Kansas and Missouri offices of the U.S. Attorney and State Attorney General conduct a training seminar in Kansas City. More than 1800 officers have attended these seminars, representing more than 680 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program.[47] The staff creates preliminary investigative reports by examining significant patterns of identity theft activity in the Clearinghouse and refining the data through the use of additional investigative resources. Then the staff refers the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers throughout the country for further investigation and potential prosecution. The FTC is aided in this work by its federal law enforcement partners, including the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service. Recently, an FBI analyst has worked intensively with the Clearinghouse complaints, using sophisticated analytical software to find related complaints and combine the information with other data sources available to the FBI.

C. Outreach and Education

The Identity Theft Act also directed the FTC to educate consumers about identity theft. Recognizing that law enforcement and private industry each play an important role in helping consumers both to minimize their risk and to recover from identity theft, the FTC expanded its outreach and education mission to include these sectors.

(1) *Consumers:* The FTC has taken the lead in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print and online materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which includes the publications and links to tes-

---

[45] Other government agencies, including the Social Security Administration, the SEC, and the FDIC, also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name.*

[46] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

[47] The referral program complements the regular use of the database by all law enforcers from their desktop computers.

timony, reports, press releases, identity theft-related state laws, and other resources.

To increase awareness for the average consumer and provide tips for minimizing the risk of identity theft, the FTC developed a new primer on identity theft, *ID Theft: What's It All About?*.[48] Taken together with the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the two publications help to educate consumers.

(2) *Law Enforcement:* Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described previously (*see infra* Section V.B), the staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. Other outreach initiatives include: (i) participation in a "Roll Call" video produced by the Secret Service, which has been sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (ii) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations.

(3) *Industry:* The private sector can help with the problem of identity theft in several ways. From prevention through better security and authentication, to helping victims recover, businesses play a key role in reducing the impact of identity theft.

(a) *Information Security Breaches:* The FTC works with institutions that maintain personal information to identify ways to help keep that information safe from identity theft.[49] In 2002, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance.[50] To provide standardized assistance in these types of cases, the FTC developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that is available on the identity theft website. The kit provides advice on contacting consumers, law enforcement agencies, business contact information for the three major credit reporting agencies, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know to protect themselves from identity theft.

(b) *Victim Assistance:* Identity theft victims may spend substantial time and effort restoring their good names and financial records. As a result, the FTC devotes substantial resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[51] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001

---

[48] Since its release in May 2003, the FTC has distributed more than 972,000 paper copies and over 119,300 web versions, and developed a Spanish version.

[49] The Commission also has law enforcement authority relating to information security. In addition to developing the Disposal Rule pursuant to FACTA, *see supra* Section IV, the Commission also is responsible for enforcing its GLBA Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. FTC Safeguards Rule, 16 C.F.R. § 314.1 (2002). In brief, the Safeguards Rule requires financial institutions to develop a written information security plan that includes certain elements that are basic to security.

In the past few years, the FTC has also brought enforcement actions against four companies that the Commission alleged made false promises about securing sensitive consumer information, in violation of Section 5 of the FTC Act. 15 U.S.C. § 45(a). These actions resulted in settlements with those companies that collected sensitive information from consumers while making such promises. Those actions arose out of the Commission's finding that these companies' security measures were inadequate and their information security claims therefore were deceptive. *See, e.g., In re Microsoft Corp.*, FTC Dkt. C-4069, Final Decision and Order available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf at (Dec. 20, 2002).

[50] *See, e.g.*, the incidents involving TriWest (Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12) and Ford/Experian (Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1).

[51] *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

through April 2004, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been more than 643,000 hits to the Web version. The affidavit is available in both English and Spanish.

VI. CONCLUSION

Identity theft places substantial costs on individuals and businesses. The Commission looks forward to working with businesses on better ways for them to protect the valuable information of consumers with which they are entrusted as well as other means of preventing identity theft. The Commission anticipates that as the new provisions of FACTA take effect, they will further help to reduce identity theft as well as its impact on victims.

Mr. STEARNS. Thank you, Commissioner.

Ms. Bovbjerg.

STATEMENT OF BARBARA D. BOVBJERG

Ms. BOVBJERG. Thank you, Mr. Chairman, Ms. Schakowsky. I am pleased to be here today to discuss issues associated with the use and misuse of the Social Security number.

Although the SSN was originally created as a means to track workers' earnings and eligibility for Social Security benefits, today the numbers are used for many non-Social Security purposes in both the public and the private sectors. This wide use of SSNs cause us concern because these numbers are among the personal identifiers most sought by identity thieves.

Today, I will present results of our work on a variety of issues associated with the SSN. I would like to focus mainly on private sector use of the SSN and the protections that private companies apply and then more briefly on public sector uses and protections. My testimony is based on reports we have prepared over the last several years on this topic.

First, the SSN and the private sector. We reported last January that consumer reporting agencies, health care organizations and information resellers use the SSN for a variety of purposes, only some of which are restricted by law, and virtually all of these entities have come to rely on the SSN as an identifier. Some businesses use the SSN to facilitate activities by assessing credit risk, locating bankruptcy assets or tracking patient care. For example, consumer reporting agencies, or CRAs, build and maintain credit histories around individuals' names, addresses, and SSNs. CRAs obtain SSNs from individuals who seek credit and from information resellers and public records. The SSNs are combined with information about a consumer's financial transactions such as charges, loans and credit repayments to ensure the consumer account data are matched correctly.

Some businesses that function as information resellers aggregate information, including SSNs, from various public and private sources for resale. They obtain data from public records like bankruptcy proceedings, tax liens and voter registration rolls and from private compilations like phone books. These businesses resell this information to a variety of customers.

Those we contacted told us that, to comply with current law, they limit their services to customers who establish accounts with them and with whom they have contracts that restrict the extent to which the data purchased can be redisclosed. Many say they truncate the SSN if they provide it all.

Indeed, Federal and State laws have helped to control access to and distribution of personal information like the SSN. At the Federal level, the Fair Credit Reporting Act, Gramm-Leach-Bliley and HIPAA, among others, have restricted use, distribution and display of the SSN in specific industries. Several States, most notably California, have enacted laws restricting display and use of SSNs; and although these are limited to a particular State, such restrictions have caused some private companies to alter their policies nationwide. No law, however, restricts use and display of the SSN in all industries in all locations, leaving the potential for misuse when protections are inadequate.

Let me turn now to the public sector. As we have reported previously, Federal, State and county government agencies rely extensively on the SSN to maintain records with unique identifiers and maintain program integrity. Although government agencies told us of the various steps they take to safeguard the SSNs they use, we found the key protections are not uniformly in place. For example, some Federal agencies and many of the State and county agencies maintain public records that contain SSNs.

Public records are documents routinely made available to the public for inspection, such as marriage licenses and property transactions, and represent a primary source of data for information resellers. GAO has expressed concern that such records create opportunities for identity thieves and has called on government at all levels to consider better protections.

In conclusion, although SSNs are used for many beneficial purposes, the widespread use and retention of SSNs in both the public and private sectors creates opportunities for identity theft. Although both government and private companies have strengthened their protections of personal data and have reduced display of this information, these actions are far from uniform and leave troubling gaps. Nonetheless, restrictions on SSN use and the protections that would ensue must be weighed against the effect of such measures on governments and businesses now reliant on the SSN.

I welcome this committee's interest on this important policy area and look forward to helping to provide information and analysis needed to assure that America's personal information is safe and secure. I thank you for your attention, and I would be happy to answer any questions you have.

[The prepared statement of Barbara D. Bovbjerg follows:]

PREPARED STATEMENT OF BARBARA D. BOVBJERG, DIRECTOR, EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE

Mr. Chairman and Members of the Subcommittee: I am pleased to be here today to discuss private and public sector entities' use of Social Security numbers (SSNs). Although the Social Security Administration (SSA) originally created SSNs as a means to track workers' earnings and eligibility for Social Security benefits, over time the SSN has come to be used for a myriad of purposes; individuals are frequently asked to supply personal information, including their SSNs, to both public and private sector entities. In addition, individuals' SSNs can be found in a number of public sources such as records displayed to the public. Given the uniqueness and broad applicability of the SSN, many private and public sector entities rely extensively on the SSN sometimes as a way to accumulate and identify information for their databases, sometimes to comply with federal regulations, and other times for various business purposes. The potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs.

Although Congress has passed a number of laws to protect the security of personal information, the continued use of and reliance on SSNs by both private and public sector entities underscores the importance of determining if appropriate safeguards are in place to protect individuals' private information or if enhanced protection of individuals' personal information is needed. Accordingly, you asked us to talk about how certain types of private and public sector entities obtain SSNs and what protections, if any, exist to govern their use. My remarks today will focus on describing (1) how private sector entities obtain, use, and protect SSNs and (2) public sector uses and protections.

To determine how private sector entities obtain, use, and protect SSNs, we relied on our previous work that looked at how private sector entities obtain and use SSNs and the laws that limit disclosure of this use.[1] To determine how the public sector uses and protects SSNs, we also relied on our previous work that looked at the government's use and protection of SSNs.[2] In addition, we are conducting structured interviews of federal agencies concerning the display of SSNs.

In summary, entities such as information resellers, consumer reporting agencies (CRAs), and health care organizations routinely obtain SSNs from their business clients and from public sources, such as marriage licenses, paternity determinations, and professional licenses. Businesses use SSNs for various purposes, such as to build databases, verify individuals' identities, or match existing records.[3] Given the various types of services these companies offer, we found that all of these entities have come to rely on the SSN as an identifier, which they say helps them determine a person's identity for the purpose of providing the services they offer. However, certain federal laws have helped to limit the disclosures of personal information these private sector entities are allowed to make to their customers. Private sector entities are either subject to the laws directly, given the nature of their business, or indirectly, through their business clients who are subject to these laws. Some states have also enacted laws to restrict the private sector's use of SSNs. However, such restrictions vary by state.

Public sector entities also rely extensively on SSNs. These agencies often obtain SSNs for compliance with federal laws and regulations and for their own agencies' purposes. We found that federal, state, and county government agencies rely extensively on the SSN to manage records, verify benefit eligibility, collect outstanding debt, conduct research and program evaluations, and verify information provided to state drivers' licensing agencies.[4] Given that SSNs are often the identifier of choice among individuals seeking to create false identities, these agencies are taking steps to safeguard SSNs. Yet despite these actions, SSNs appear in records displayed to the public such as documents that record financial transactions or court documents. In a previous report, we proposed that Congress consider developing a unified approach to safeguarding SSNs used in all levels of government and particularly those displayed in public records, and we continue to believe that this approach has merit.[5]

BACKGROUND

The Social Security Act of 1935 authorized SSA to establish a record-keeping system to help manage the Social Security program, and this resulted in the creation of the SSN. Through a process known as enumeration, unique numbers are created for every person as a work and retirement benefit record for the Social Security program. SSA generally issues SSNs to most U.S. citizens, and SSNs are also available to noncitizens lawfully admitted to the United States with permission to work. SSA estimates that approximately 277 million individuals currently have SSNs. The SSN has become the identifier of choice for government agencies and private businesses, and thus it is used for a myriad of non-Social Security purposes.

The growth in the use of SSNs is important to individual SSN holders because these numbers, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves.[6] In addition, SSNs are used as breeder information to create additional false identification documents, such as drivers' licenses. Recent statistics collected by federal agencies and CRAs indicate

---

[1] *GAO, Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information,* GAO-04-11 (Washington D.C.: January 22, 2004).

[2] See GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards,* GAO-02-352 (Washington, D.C.: May 31, 2002).

[3] GAO-04-11 (Washington D.C.: January 2004).

[4] GAO-02-352 (Washington D.C.: May 2002).

[5] GAO-02-352 (Washington D.C.: May 2002).

[6] United States Sentencing Commission, *Identity Theft Final Alert* (Washington, D.C.: Dec. 15, 1999).

that the incidence of identity theft appears to be growing.[7] The Federal Trade Commission (FTC), the agency responsible for tracking identity theft, reported that consumer fraud and identity theft complaints grew from 404,000 in 2002 to 516,740 in 2003. In 2003, consumers also reported losses from fraud of more than $437 million, up from $343 million in 2002. In addition, identity crimes account for over 80 percent of SSN misuse allegations according to the SSA. Also, officials from two of the three national CRAs report an increase in the number of 7-year fraud alerts placed on consumer credit files, which they consider to be reliable indicators of the incidence of identity theft.[8] Law enforcement entities report that identity theft is almost always a component of other crimes, such as bank fraud or credit card fraud, and may be prosecuted under the statutes covering those crimes.

PRIVATE SECTOR ENTITIES ROUTINELY OBTAIN AND USE SSNS, AND CERTAIN LAWS AFFECT THE DISCLOSURE OF THIS INFORMATION

Private sector entities such as information resellers, CRAs, and health care organizations routinely obtain and use SSNs.[9] Such entities obtain the SSNs from various public sources and their business clients wishing to use their services. We found that these entities usually use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. Certain federal laws have limited the disclosures private sector entities are allowed to make to their customers, and some states have also enacted laws to restrict the private sector's use of SSNs.

Private Sector Entities Obtain SSNs from Public and Private Sources and Use SSNs for Various Purposes

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources and use SSNs to help identify individuals. Of the various public sources available, large information resellers told us they obtain SSNs from various records displayed to the public such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registrations, and professional licenses. Large information resellers said that they try to obtain SSNs from public sources where possible, and to the extent public record information is provided on the Internet, they are likely to obtain it from such sources. Some of these officials also told us that they have people that go to courthouses or other repositories to obtain hard copies of public records. Additionally, they obtain batch files of electronic copies of all public records from some jurisdictions.

Given the varied nature of SSN data found in public records, some reseller officials said they are more likely to rely on receiving SSNs from their business clients than they are from obtaining SSNs from public records. These entities obtain SSNs from their business clients, who provide SSNs in order to obtain a reseller's services or products, such as background checks, employee screening, determining criminal histories, or searching for individuals. Large information resellers also obtain SSN information from private sources. In many cases such information was obtained through review of data where a customer has voluntarily supplied information resellers with information about himself or herself. In addition, large reseller officials said they also use their clients' records in instances where the client has provided them with information.

We also found that Internet-based resellers rely extensively on public sources and records displayed to the public. These resellers listed on their Web sites public information sources, such as newspapers, and various kinds of public record sources at the county, state, and national levels. During our investigation, we determined that once Internet-based resellers obtained an individual's SSN they relied on information in public records to help verify the individual's identity and amass information around the individual's SSN.

---

[7] GAO, *Identity Theft: Prevalence and Cost Appeor to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

[8] A fraud alert is a warning that someone may be using the consumer's personal information to fraudulently obtain credit. When a fraud alert is placed on a consumer's credit card file, it advises credit grantors to conduct additional identity verification before granting credit. The three consumer reporting agencies offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

[9] Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information that includes SSNs for informational services. CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Health care organizations generally deliver their services through a coordinated system that includes health care providers and health plans, also referred to as health care insurers.

Like information resellers, CRAs also obtain SSNs from public and private sources as well as from their customers or the businesses that furnish data to them. CRA officials said that they obtain SSNs from public sources, such as bankruptcy records, a fact that is especially important in terms of determining that the correct individual has declared bankruptcy. CRA officials also told us that they obtain SSNs from other information resellers, especially those that specialize in obtaining information from public records. However, SSNs are more likely to be obtained from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Individuals provide these businesses with their SSNs for reasons such as applying for credit, and these businesses voluntarily report consumers' charge and payment transactions, accompanied by SSNs, to CRAs.

We found that health care organizations were less likely to rely on public sources for SSN data. Health care organizations obtain SSNs from individuals themselves and from companies that offer health care plans. For example, subscribers or policyholders provide health care plans with their SSNs through their company or employer group when they enroll in health care plans. In addition to health care plans, health care organizations include health care providers, such as hospitals. Such entities often collect SSNs as part of the process of obtaining information on insured people. However, health care officials said that, particularly with hospitals, the medical record number rather than the SSN is the primary identifier.

Information resellers, CRAs, and health care organization officials all said that they use SSNs to verify an individual's identity. Most of the officials we spoke to said that the SSN is the single most important identifier available, mainly because it is truly unique to an individual, unlike an individual's name and address, which can often change over an individual's lifetime. Large information resellers said that they generally use the SSN as an identity verification tool. Some of these entities have incorporated SSNs into their information technology, while others have incorporated SSNs into their clients' databases used for identity verification. For example, one large information reseller that specializes in information technology solutions has developed a customer verification data model that aids financial institutions in their compliance with some federal laws regarding "knowing your customer." We also found that Internet-based information resellers use the SSN as a factor in determining an individual's identity. We found these types of resellers to be more dependent on SSNs than the large information resellers, primarily because their focus is more related to providing investigative or background-type services to anyone willing to pay a fee. Most of the large information resellers officials we spoke to said that although they obtain the SSN from their business clients, the information they provide back to their customers rarely contains the SSN. Almost all of the officials we spoke to said that they provide their clients with a truncated SSN, an example of which would be xxx-xx-6789.

CRAs use SSNs as the primary identifier of individuals, which enables them to match the information they receive from their business clients with the information stored in their databases on individuals.[10] Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly with an individual's information on file. For example, CRA officials said they use several factors to match incoming data with existing data, such as name, address, and financial account information. If all of the incoming data, except the SSN, match with existing data, then the SSN will determine the correct person's credit file. Given that people move, get married, and open new financial accounts, these officials said that it is hard to distinguish among individuals. Because the SSN is the one piece of information that remains constant, they said that it is the primary identifier that they use to match data.

Health care organizations also use the SSN to help verify the identity of individuals. These organizations use SSNs, along with other information, such as name, address, and date of birth, as a factor in determining a member's identity. Health care officials said that health care plans, in particular, use the SSN as the primary identifier of an individual, and it often becomes the customer's insurance number. Health care officials said that they use SSNs for identification purposes, such as linking an individual's name to an SSN to determine if premium payments have

[10] We found that CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinction between the two types of businesses but does not affect the use of SSNs by these entities. Five of the six large information resellers we spoke to said they were also CRAs. Some CRA officials said that information reselling constituted as much as 40 percent of CRAs' business.

been made. They also use the SSN as an online services identifier, as an alternative policy identifier, and for phone-in identity verification. Health care organizations also use SSNs to tie family members together where family coverage is used,[11] to coordinate member benefits, and as a cross-check for pharmacy transactions. Health care industry association officials also said that SSNs are used for claims processing, especially with regard to Medicare. According to these officials, under some Medicare programs, SSNs are how Medicare identifies benefits provided to an individual.

Certain Laws Limit the Private Sectors' Disclosure of Personal Information That Includes SSNs

Certain federal and state laws have placed restrictions on certain private sector entities use and disclosure of consumers' personal information that includes SSNs. Such laws include the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in table 1, the laws either restrict the disclosures that entities such as information resellers, CRAs, and health care organizations are allowed to make to specific purposes or restrict whom they are allowed to give the information to. Moreover, as shown in table 1, these laws focus on limiting or restricting access to certain personal information and are not specifically focused on information resellers. See appendix I for more information on these laws.

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal Laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to non-affiliated third parties.
Drivers Privacy Protection Act	Prohibits obtaining and disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law.
Health Insurance Portability and Accountability Act.	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis.

We reviewed selected legislative documents of 18 states and found that at least 6 states have enacted their own legislation to restrict either the display or use of SSNs by the private sector.[12] Notably, in 2001, California enacted Senate Bill (SB) 168, restricting private sector use of SSNs. Specifically, this law generally prohibits companies and persons from certain uses such as, posting or publicly displaying SSNs and printing SSNs on cards required to access the company's products or services. Furthermore, in 2002, shortly after the enactment of SB 168, California's Office of Privacy Protection published recommended practices for protecting the confidentiality of SSNs. These practices were to serve as guidelines to assist private and public sector organizations in handling SSNs.

Similar to California's law, Missouri's law (2003 Mo. SB 61), which is not effective until July 1, 2006, bars companies from requiring individuals to transmit SSNs over the Internet without certain safety measures, such as encryption and passwords. However, while SB 61 prohibits a person or private entity from publicly posting or displaying an individual's SSN "in any manner," unlike California's law, it does not specifically prohibit printing the SSN on cards required to gain access to products or services. In addition, Arizona's law (2003 Ariz. Sess. Laws 137), effective January 1, 2005, restricts the use of SSNs in ways very similar to California's law. However, in addition to the private sector restrictions, it adds certain restrictions for state

[11] During the enrollment process, subscribers have a number of options, one of which is decided whether they would like single or family coverage. In cases where family coverage is chosen, the SSN is the key piece of information generally allowing the family members to be linked.

[12] On the basis of our interviews with private sector businesses and organizations, contacts with some state offices of attorney general, and identification of state laws and legislative initiatives related to the use of SSNs, we did a legislative review of 18 states that were identified as having laws or proposed laws governing SSN use. In the 18 states we researched, we reviewed more than 40 legislative documents, including relevant laws, proposed laws, legislative summaries, and other related documents, such as state regulations, executive orders, and referendums.

agencies and political subdivisions.[13] For example, state agencies and political subdivisions are prohibited from printing an individual's SSN on cards and certain mailings to the individual. Last, Texas prohibits the display of SSNs on all cards, while Georgia and Utah's laws are directed at health insurers and, therefore, pertain primarily to insurance identification cards.[14] None of these three laws contain the provisions mentioned above relating to Internet safety measures and mailing restrictions. Table 2 lists states that have enacted legislation and related provisions.

Table 2: Provisions Included in Enacted Legislation Reviewed

Provision	States Where Provision or Restriction Enacted
Specifically prohibits display on cardsgDAZ, CA, GA, TX, UT.	
Requires Internet safety measures	AZ, CA, MO
Restricts mailing of SSNs	AZ, CA

Source: GAO analysis.

PUBLIC SECTOR ENTITIES ALSO USE SSNS AND SOME AGENCIES LIMIT THEIR USE AND DISPLAY

Agencies at all levels of government frequently obtain and use SSNs. A number of federal laws require government agencies to obtain SSNs, and these agencies use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and do research and evaluation. In addition, given the open nature of certain government records, SSNs appear in some records displayed to the public. Given the potential for misuse, some government agencies are taking steps to limit their use and display of SSNs and prevent the proliferation of false identities.

Public Sector Entities Are Required by Laws and Regulations to Obtain SSNs and Use SSNs for Various Purposes

Government agencies obtain SSNs because a number of federal laws and regulations require certain programs and federally funded activities to use the SSN for administrative purposes.[15] Such 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. For example, the Internal Revenue Code and regulations, which govern the administration of the federal personal income tax program, require that individuals' SSNs serve as taxpayer identification numbers.[16] A number of other federal laws require program administrators to use SSNs in determining applicants' eligibility for federally funded benefits. The Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, Food Stamp, Temporary Assistance for Needy Families, and Medicaid programs.[17] In addition, the Commercial Motor Vehicle Safety Act of 1986 requires the use of SSNs to identify individuals and established the Commercial Driver's License Information System, a nationwide database where states may use individuals' SSNs to search the database for other state-issued licenses commercial drivers may hold.[18] Federal law also requires the use of SSNs in state child support programs to help states locate noncustodial parents, establish and enforce support orders, and recoup state welfare payments from par-

[13] Political subdivisions would include counties, cities, and towns.

[14] Georgia's law (O.C.G.A. §33-24-57.1(f)) and Utah's law (Utah Code Ann. §31-22-634) were both effective July 1, 2004. However, Utah's law provides certain extensions until March 1, 2005. Texas' law (2003 Tex. Gen. Laws 341) is effective March 1, 2005.

[15] GAO, *Social Security Numbers: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington D.C.: February 1999).

[16] This means that employers and others making payments to individuals must include the individuals' SSNs in reporting to IRS many of these payments. In addition, the Code and regulations require individuals filing personal income tax returns to include their SSNs as their taxpayer identification number, the SSNs of people whom they claim as dependents, and the SSNs of spouses to whom they paid alimony.

[17] Applicants give program administrators information on their income and resources, and program administrators use applicants' SSNs to match records with those of other organizations.

[18] States may also use SSNs to search another database, the National Driver's Registry, to determine whether an applicant's license has been cancelled, suspended, or revoked by another state. In these situations, the states use SSNs to limit the possibility of inappropriately licensing applicants.

ents.[19] The law also requires states to record SSNs on many other state documents, such as professional, occupational, and marriage licenses; divorce decrees; paternity determinations; and death certificates.

Government agencies use SSNs for a variety of reasons. We found that most of these agencies use SSNs to administer their programs, such as to identify, retrieve, and update their records. In addition, many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. As unique identifiers, SSNs help ensure that the agency is obtaining or matching information on the correct person.

Government agencies also share information containing SSNs for the purpose of verifying an applicant's eligibility for services or benefits, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments. SSNs are also used to ensure program integrity. Agencies use SSNs to collect delinquent debts and even share information for this purpose. In addition, SSNs are used for statistics, research, and evaluation. Agencies responsible for collecting and maintaining data for statistical programs that are required by statute, make use of SSNs. In some cases, these data are compiled using information provided for another purpose. For example, the Bureau of the Census prepares annual population estimates for states and counties using individual income tax return data linked over time by SSN to determine immigration rates between localities.[20] SSNs also provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources to help evaluate the outcomes or effectiveness of government programs. In some cases, records containing SSNs are sometimes matched across multiple agency or program databases.[21]

Government agencies also use employees' SSNs to fulfill some of their responsibilities as employers. For example, personnel departments of these agencies use SSNs to help them maintain internal records and provide employee benefits. In addition, employers are required by law to use employees' SSNs when reporting wages. Wages are reported to SSA, and the agency uses this information to update earnings records it maintains for each individual. The Internal Revenue Service (IRS) also uses SSNs to match the employer wage reports with amounts individuals report on personal income tax returns. Federal law also requires that states maintain employers' reports of newly hired employees, identified by SSNs. States must forward this information to a national database that is used by state child support agencies to locate parents who are delinquent in child support payments.

Finally, SSNs appear in some government records that are open to the public. For example, SSNs may already be a part of a document that is submitted to a recorder for official preservation, such as veterans' discharge papers. Documents that record financial transactions, such as tax liens and property settlements, also contain SSNs to help identify the correct individual. Government officials are also required by law to collect SSNs in numerous instances, and some state laws allow government entities to collect SSNs on voter registries to help avoid duplicate registrations. In addition, courts at all three levels of government also collect and maintain records that are routinely made available to the public. SSNs appear in court documents for a variety of reasons such as on documents that government officials create like criminal summonses, and in many cases, SSNs are already a part of documents that are submitted by attorneys or individuals as part of the evidence for a proceeding or a petition for an action. In some cases, federal law requires that SSNs be placed in certain records that courts maintain, such as child support orders.

Government Agencies Are Taking Steps to Limit the Use and Display of SSNs

Despite the widespread use of SSNs at all levels of government, not all agencies use SSNs. We found that some agencies do not obtain, receive, or use SSNs of program participants, service recipients, or individual members of the public.[22] Moreover, not all agencies use the SSN as their primary identification number for record-

[19] The law requires states to maintain records that include (1) SSNs for individuals who owe or are owed support for cases in which the state has ordered child support payments to be made, the state is providing support, or both, and (2) employers' records of new hires identified by SSN.

[20] The Bureau of the Census is authorized by statute to collect a variety of information, and the Bureau is also prohibited from making it available, except in certain circumstances.

[21] The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See U.S. General Accounting Office, *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*, GAO-01-126SP (Washington, D.C.: Apr. 2001).

[22] GAO-02-352 (Washington D.C.: May 2002).

keeping purposes. These agencies maintain an alternative number that is used in addition to or in lieu of SSNs for certain activities.

Some agencies are also taking steps to limit SSNs displayed on documents that may be viewed by others who may not have a need to view this personal information. For example, the Social Security Administration has truncated individuals' SSNs that appear on the approximately 120 million benefits statements it mails each year. Some states have also passed laws prohibiting the use of SSNs as a student identification number. Almost all states have modified their policies on placing SSNs on state drivers' licenses.

At the federal level, SSA has taken steps in its enumeration process and verification service to help prevent SSNs from being used to proliferate false identities. SSA has formed a task force to address weaknesses in its enumeration process and has (1) increased document verifications and developed new initiatives to prevent the inappropriate assignment of SSNs to noncitizens, and (2) undertaken initiatives to shift the burden of processing noncitizen applications from its field offices.[23] SSA also helps prevent the proliferation of false identities through its verification service, which allows state driver licensing agencies to verify the SSN, name, and date of birth of customers with SSA's master file of Social Security records.[24] Finally, SSA has also acted to correct deficiencies in its information systems' internal controls. These changes were made in response to the findings of an independent audit that found that SSA's systems were exposed to both internal and external intrusion, increasing the possibility that sensitive information such as SSNs could be subject to unauthorized access, modification, and disclosure, as well as the risk of fraud.

With regard to the courts, in a prior report we suggested that Congress consider addressing SSN security and display issues in state and local government and in public records, including those maintained by the judicial branch of government at all levels.[25] We proposed that Congress convene a representative group of officials from all levels of government to develop a unified approach to safeguard SSNs used in all levels of government and particularly those displayed in public records.

CONCLUSIONS

Public and private entities use SSNs for many legitimate and publicly beneficial purposes. However, the more frequently SSNs are obtained and used, the more likely they are to be misused. Individuals may voluntarily provide their SSNs to the private and public sectors to obtain services, but they should be able to be confident that their personal information is safe and secure. As we continue to learn more about the entities that obtain SSNs and the purposes for which they obtain them, policy makers will be able to determine if there are ways to limit access to this valuable piece of information and prevent it from being misused. However, restrictions on access or use may make it more difficult for businesses and government agencies to verify an individual's identity. Accordingly, policy makers will have to balance the potential benefits of restrictions on the use of SSNs on the one hand with the impact on legitimate needs for the use of SSNs on the other.

We are continuing our work on protecting the privacy of SSNs in the private and public sectors, and we are pleased that this Subcommittee is considering this important policy issue. That concludes my testimony, and I would be pleased to respond to any questions the subcommittee has.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director or Tamara Cross, Assistant Director at (202) 512-7215.

APPENDIX I: FEDERAL LAWS AFFECTING INFORMATION RESELLERS, CRAS, AND HEALTH CARE ORGANIZATIONS:

GRAMM-LEACH-BLILEY ACT (GLBA):

GLBA requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information. Financial institu-

[23] See *GAO, Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens but Some Weakness Remain,* GAO-04-12 (Washington D.C.: October 15, 2003). See GAO, *Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification,* GAO-03-920 (Washington D.C.: September 15, 2003).

[24] GAO-03-920 (Washington D.C.: September 2003).

[25] GAO-02-352 (Washington D.C.: May 2002)

tions are permitted to disclose consumers' nonpublic personal information without offering them an opt-out right in the following circumstances:

- to effect a transaction requested by the consumer in connection with a financial product or service requested by the consumer; maintaining or servicing the consumer's account with the financial institution or another entity as part of a private label credit card program or other extension of credit; or a proposed or actual securitization, secondary market sale, or similar transaction;
- with the consent or at the direction of the consumer;
- to protect the confidentiality or security of the consumer's records; to prevent actual or potential fraud, for required institutional risk control or for resolving customer disputes or inquiries, to persons holding a legal or beneficial interest relating to the consumer, or to the consumer's fiduciary;
- to provide information to insurance rate advisory organizations, guaranty funds or agencies, rating agencies, industry standards agencies, and the institution's attorneys, accountants, and auditors;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;
- to a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency;
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business if the disclosure concerns solely consumers of such business;
- to comply with federal, state, or local laws; an investigation or subpoena; or to respond to judicial process or government regulatory authorities.

Financial institutions are required by GLBA to disclose to consumers at the initiation of a customer relationship, and annually thereafter, their privacy policies, including their policies with respect to sharing information with affiliates and nonaffiliated third parties.

Provisions under GLBA place limitations on financial institutions disclosure of customer data, thus affecting some CRAs and information resellers. We found that some CRAs consider themselves to be financial institutions under GLBA.[26] These entities are therefore directly governed by GLBA's restrictions on disclosing nonpublic personal information to non-affiliated third parties. We also found that some of the information resellers we spoke to did not consider their companies to be financial institutions under GLBA. However, because they have financial institutions as their business clients, they complied with GLBA's provisions in order to better serve their clients and ensure that their clients are in accordance with GLBA. For example, if information resellers received information from financial institutions, they could resell the information only to the extent that they were consistent with the privacy policy of the originating financial institution.

Information resellers and CRAs also said that they protect the use of non-public personal information and do not provide such information to individuals or unauthorized third parties. In addition to imposing obligations with respect to the disclosures of personal information, GLBA also requires federal agencies responsible for financial institutions to adopt appropriate standards for financial institutions relating to safeguarding customer records and information. Information resellers and CRA officials said that they adhere to GLBA's standards in order to secure financial institutions' information.

DRIVERS PRIVACY PROTECTION ACT (DPPA):

The DPPA specifies a list of exceptions when personal information contained in a state motor vehicle record may be obtained and used (18 U.S.C. § 2721(b)). These permissible uses include:

- for use by any government agency in carrying out its functions;
- for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; motor vehicle market research activities, including survey research;
- for use in the normal course of business by a legitimate business, but only to verify the accuracy of personal information submitted by the individual to the business and, if such information is not correct, to obtain the correct informa-

[26] Under GLBA, the term financial institution is defined as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956," which goes into more detail about what are "activities that are financial in nature." These generally include banking, insurance, and investment industries.

tion but only for purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual;
- for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency;
- for use in research activities;
- for use by any insurer or insurance support organization in connection with claims investigation activities;
- for use in providing notice to the owners of towed or impounded vehicles;
- for use by a private investigative agency for any purpose permitted under the DPPA;
- for use by an employer or its agent or insurer to obtain information relating to the holder of a commercial driver's license;
- for use in connection with the operation of private toll transportation facilities;
- for any other use, if the state has obtained the express consent of the person to whom a request for personal information pertains;
- for bulk distribution of surveys, marketing, or solicitations, if the state has obtained the express consent of the person to whom such personal information pertains;
- for use by any requester, if the requester demonstrates that it has obtained the written consent of the individual to whom the information pertains;
- for any other use specifically authorized under a state law, if such use is related to the operation of a motor vehicle or public safety.

As a result of DPPA, information resellers said they were restricted in their ability to obtain SSNs and other driver license information from state motor vehicle offices unless they were doing so for a permissible purpose under the law. These officials also said that information obtained from a consumer's motor vehicle record has to be in compliance with DPPA's permissible purposes, thereby restricting their ability to resell motor vehicle information to individuals or entities not allowed to receive such information under the law. Furthermore, because DPPA restricts state motor vehicle offices' ability to disclose driver license information, which includes SSN data, information resellers said they no longer try to obtain SSNs from state motor vehicle offices, except for permissible purposes.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA):

The HIPAA privacy rule also defines some rights and obligations for both covered entities and individual patients and health plan members. Some of the highlights are:
- Individuals must give specific authorization before health care providers can use or disclose protected information in most nonroutine circumstances, such as releasing information to an employer or for use in marketing activities.
- Covered entities will need to provide individuals with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to individuals choosing a health plan, doctor, or other service provided. Patients will be generally asked to sign or otherwise acknowledge receipt of the privacy notice.

Covered entities must obtain an individual's specific authorization before sending them marketing materials.

Health care organizations, including health care providers and health plan insurers, are subject to HIPAA's requirements. In addition to providing individuals with privacy practices and notices, health care organizations are also restricted from disclosing a patient's health information without the patient's consent, except for purposes of treatment, payment, or other health care operations. Information resellers and CRAs did not consider themselves to be "covered entities" under HIPAA, although some information resellers said that their customers are considered to be business associates under HIPAA. As a result, they said they are obligated to operate under HIPAA's standards for privacy protection, and therefore could not resell medical information without having made sure HIPAA's privacy standards were met.

FAIR CREDIT REPORTING ACT (FCRA):

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report (15 USC 1681b). These permissible purposes are:
- as ordered by a court or a federal grand jury subpoena;
- as instructed by the consumer in writing;
- for the extension of credit as a result of an application from a consumer or the review or collection of a consumer's account;

- for employment purposes, including hiring and promotion decisions, where the consumer has given written permission;
- for the underwriting of insurance as a result of an application from a consumer;
- when there is a legitimate business need, in connection with a business transaction that is initiated by the consumer;
- to review a consumer's account to determine whether the consumer continues to meet the terms of the account;
- to determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;
- for use by a potential investor or servicer or current insurer in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation; and
- for use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof.

Under FCRA, Congress has limited the use of consumer reports[27] to protect consumers' privacy and limits access to credit data to those who have a legally permissible purpose for using the data, such as the extension of credit, employment purposes, or underwriting insurance. However, these limits are not specific to SSNs. All of the CRAs that we spoke to said that they are considered consumer reporting agencies under FCRA. In addition, some of the information resellers we spoke to who handle or maintain consumer reports are classified as CRAs under FCRA. Both CRAs and information resellers said that as a result of FCRAs restrictions they are limited to providing credit data to their customers that have a permissible purpose under FCRA. Consequently, they are restricted by law from providing such information to the general public.

Mr. STEARNS. I thank you.

Mr. Hoofnagle.

STATEMENT OF CHRIS JAY HOOFNAGLE

Mr. HOOFNAGLE. Thank you, Chairman Stearns and Ranking Member Schakowsky, for this opportunity today to speak about the privacy of Social Security numbers.

My name is Chris Hoofnagle, and I am Associate Director with the Electronic Privacy Information Center here in Washington, D.C. We were established in 1994 to protect privacy, the first amendment and constitutional values. Since our founding in 1994, we have been active in trying to protect the Social Security number.

As you are well aware, today the Social Security number plays an unparalleled role in the identification, authentication and tracking of Americans. This widespread use exacerbates several privacy problems. Since it is used as both an identifier and an authenticator, that is, some businesses use it as a record locator or a way to amass personal information about individuals, other businesses use it as a password, and that creates many of the problems that we are experiencing today in identity theft and privacy more generally.

Serious security problems are raised in any system where a single device is used as both identifier and password. Just imagine if your bank account assigned you an account number and a PIN that were the same. Anyone who was able to recover a cashed check or one of your account statements could very easily plunder your account or in a similar situation when it comes to the SSN. Because the SSN is used in this way so prevalently in the public and private sector, it is so relied upon by business, it has become the iden-

[27] The FTC has determined that certain types of information, including SSNs, do not constitute as consumer report under FCRA because they are not factors in determining credit eligibility.

tifier that criminals use when they want to commit fraud and identity theft.

There is now a rich history in identity theft litigation showing that the crime is exacerbated by creditors who issue new accounts based on an SSN match alone. Creditors are ignoring incorrect information on credit applications and granting credit even where the SSN matches but other critical pieces of information such as name, date of birth and address do not match.

In May, the Salt Lake Tribune reported that businesses granting credit did little to ensure that Social Security numbers and names match. The same newspaper argued there are credit bureaus that allow perpetrators to establish credit files using other people's Social Security numbers. That article also reports on an inspector general from the Social Security Administration, who then at the time stated that SSN-only fraud makes up the majority of cases of identity theft in Utah and the surrounding region. We think this is further evidence that there needs to be less reliance on the Social Security number and more care in credit transactions in particular.

But let me be clear about this. This in no way threatens instant credit or access to services. All we are arguing is that greater care needs to be made available so that individuals are not able to be victimized so easily. Congress' goal in addressing identity theft and privacy issues should seek to limit the availability of the SSN generally and induce businesses to rely upon alternative identifiers.

Several provisions of H.R. 2971 are very important and should be included in any legislation considered by this committee, for instance, a prohibition on coercive disclosure. That is the practice where a business denies a service or access to a product based on a customer's withholding of the SSN. We think it is very important to address that practice.

Any Social Security number bill should also include a provision that moves the identifier below the line on a credit report. That is, a company should not be able to sell the Social Security number unless they have a valid, permissible purpose under the Fair Credit Reporting Act. H.R. 2971 does enact that protection.

I wish to highlight two important changes that should be made to the bill as amended.

First, our reading of the bill shows that Social Security numbers are only protected when the government requires their disclosure and actually states that their disclosure is mandatory. This is key to protection in a privacy act that requires the government and States to tell people whether or not disclosure of their SSN is mandatory. A lot of States are not complying with the privacy act and not telling people that they don't need to provide their SSN and, as a result, they wouldn't have protections under the bill.

We think it is important to strengthen the standards that the Attorney General will use in determining whether or not businesses should be able to use their Social Security number in the private sector. In the public sector, the SSN would be able to be disclosed where there was a compelling interest that could not be served by alternative means.

However, in the private sector, the standard is much looser. We really think that the private sector should be held to a similar standard to induce it to use alternative identifiers.

We also think that any exception that is made that allows disclosure of the SSN should be limited in time. Because if you create an exception that exists forever, businesses will solidify their use of the SSN, and they will continue to use it.

Let me conclude by thanking you for holding this hearing and continuing to develop a legislative history on the privacy of the Social Security number.

[The prepared statement of Chris Jay Hoofnagle follows:]

PREPARED STATEMENT OF CHRIS JAY HOOFNAGLE, ASSOCIATE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for extending the opportunity to testify on protecting Social Security Numbers.

My name is Chris Hoofnagle and I am associate director with the Electronic Privacy Information Center (EPIC), a not-for-profit research organization based in Washington, D.C. Founded in 1994, EPIC has participated in cases involving the privacy of the Social Security Number (SSN) before federal courts and, most recently, before the Supreme Court of New Hampshire.[1] EPIC has also taken a leading role in campaigns against the use of globally unique identifiers (GUIDs) involving the Intel Processor Serial Number and the Microsoft Corporation's Passport identification and authentication system. EPIC maintains an archive of information about the SSN online at http://www.epic.org/privacy/ssn/.

In previous testimony to Congress, EPIC has recommended a strong framework of Fair Information Practices to create rights and responsibilities for individuals and collectors of the SSN. In 2001, EPIC Executive Director Marc Rotenberg traced the history of the SSN as an identifier, highlighted the use of the SSN in the financial services sector, and raised privacy issues associated with the Social Security Administration's Death Master File.[2] In 2002, EPIC testified that the problem of identity theft had grown worse, that the states were acting to limit collection and disclosure of the SSN, and that 107 H.R. 2036, the Social Security Number Privacy and Identity Theft Protection Act of 2001 could limit misuse of the SSN.[3] In 2003, EPIC appeared again to testify in favor of privacy protections, highlighting recent abuses, the continuing unnecessary use of the SSN as an identifier by both private and public sector entities, and the developing trends of state legislation crafted to limit collection and use of the identifier.[4] In June 2004, EPIC provided an overview and recommendations for 108 H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003.[5] We testified that the bill was a good start, but could use improvement.

In today's testimony, we highlight a substitute version of 108 H.R. 2971. We make recommendations to strengthen the bill. We then cite examples of state SSN regula-

---

[1] *Estate of Helen Remsburg v. Docusearch, Inc.*, et al, C-00-211-B (N.H. 2002). In *Remsburg*, the "Amy Boyer" case, Liam Youens was able to locate and eventually murder Amy Boyer through hiring private investigators who tracked her by her date of birth, Social Security Number, and by pretexting. EPIC maintains information about the Amy Boyer case online at http://www.epic.org/privacy/boyer/.

[2] *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 (testimony of Marc Rotenberg, Executive Director, EPIC), available at http://www.epic.org/privacy/ssn/testimony—11—08—2001.html.

[3] *Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves, Joint Hearing Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims*, Sept. 19, 2002 (testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC), available at http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[4] *Hearing on Use and Misuse of the Social Security Number, Hearing Before the House Ways and Means Subcommittee on Social Security*, July 10, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, EPIC), available at http://www.epic.org/privacy/ssn/testimony7.10.03.html.

[5] *Hearing on Enhancing Social Security Number Privacy, Before the House Ways and Means Subcomm. on Social Security*, 108th Cong. (2004) (statement of Chris Hay Hoofnagle, associate director, Electronic Privacy Information Center), available at http://www.epic.org/privacy/ssn/ssntestimony6.15.04.html

tion that could be adopted at the federal level to provide an umbrella of protections for the SSN.

I. RECOMMENDATIONS FOR 108 H.R. 2971, THE SOCIAL SECURITY NUMBER PRIVACY AND IDENTITY THEFT PREVENTION ACT OF 2003

Introduced in July 2003, H.R. 2971 is the latest of a series of bills designed to enhance protections for the SSN and to promote the integrity of the identifier. It enjoys bipartisan support in the House of Representatives. The substitute measure contains many of the protections we recommended in our June 2004 testimony. However, some sections have been changed to the detriment of privacy. We highlight those sections below.

Title I of the bill sets forth limitations on government disclosure of SSNs. Broadly put, this title would prohibit executive, legislative, or judicial entities from disclosing the SSN, subject to certain exceptions.

We think it critical to make several changes to section 101. First, the legislation amends 42 U.S.C. § 405(c)(2)(C) to protects SSNs where the identifier has been given to an agency "pursuant to the assertion by such agency...that disclosure of such number is mandatory." This is a serious weakness in the bill that is keyed upon a requirement in the Privacy Act that government entities disclose whether SSN collection is mandatory or voluntary. Many state entities, in particular, do not comply with this disclosure requirement in the Privacy Act. As a result, individuals do not always understand whether SSN collection is mandatory or voluntary. Oddly, the legislation as drafted would reward agencies that didn't comply with the Privacy Act's voluntary/mandatory notice requirements by also immunizing them from prohibitions on SSN disclosure. We recommend striking this language.

We recommend removal of exemption VI in section 101, which gives credit reporting agencies wholesale access to SSNs in the hands of the government. It is not the role of government to collect SSNs from citizens, who are often under legal compulsion to provide the identifier, and then release the SSNs to the private sector for the purpose of compiling dossiers. Professor Daniel Solove has fully articulated how this model of information flow is unfair to individuals and privacy invasive:

> Imagine that the government had the power to compel individuals to reveal a vast amount of personal information about themselves—where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions, the names of their parents, children, and spouses, their political party affiliations, where they work and what they do, the property that they own and its value, and sometimes even their psychotherapists' notes, doctors' records, and financial information.
>
> Then imagine that the government routinely poured this information into the public domain—by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request. In an increasingly "wired" society, with technology such as sophisticated computers to store, transfer, search, and sort through all this information, imagine the way that the information could be combined or used to obtain even more personal information.[6]

In section 101, we recommend harmonizing the definition of "sale" (to be codified at 42 U.S.C. § 405(c)(2)(C)(x)(IX)) with other references to the term that appear in the legislation. The definition appearing in section 108, which defines sell as "to obtain, directly or indirectly, anything of value in exchange for such number," is more appropriate.

In section 101, we recommend removal of language that would allow continued disclosure of just the last four digits of the SSN, even with the six-year sunset. These last four digits are the unique portion of the SSN, and the legislation's protections are significantly weakened if this portion can sill be displayed.

Section 102 specifies the authority of the Attorney General to create exemptions to the general prohibition on government disclosure of the SSN. We agree with the standard set forth by the legislation—that SSNs should not be disclosed absent a compelling interest that cannot be served through the employment of alternative measures. *This same standard should apply to sale of the SSN to the general public.* Currently, the substitute measure would require the Attorney General to engage in

[6] Professor Daniel Solove describes this problem in *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minnesota Law Review 1137 (2002), available at http://papers.ssrn.com/sol3/papers.cfm?abstract id=283924.

a balancing test of the benefits and harms associated with the sale of the SSN to the private sector.

We think that exceptions to the general prohibition should be limited in duration. A time limit will encourage users of the SSN to transition to alternative identifiers. Exceptions that are not time limited will ensure that SSN users never transition to alternative measures.

Section 103 would codify an important safeguard—a prohibition of printing SSNs on checks issued by governments. This is a common sense protection against identity theft. It is necessary because a standard check with a SSN contains all the personal information necessary for commission of identity theft.

Section 104 would prohibit states from displaying the SSN on driver's licenses. Again, this is a common sense approach to preventing identity theft. Indeed, many states already incorporate a ban on printing the SSN on driver's licenses.[7] Such a prohibition makes it more likely that the SSN will not appear in the wallet of individuals, thus reducing the risk that a lost or stolen wallet will provide the personal information necessary to commit identity theft.

Section 106 would prohibit government entities from allowing prisoners to have access to the SSN. We think that this too is a common sense protection, in light of the Metromail case, where a company employed prisoners to enter personal information from surveys into computers. This resulted in a stalking case where a prisoner harassed a woman based on information she submitted on a survey. The woman received mail from a convicted rapist and burglar who knew everything about her—including her preferences for bath soap and magazines. The woman sued and as a result of a class-action suit, Metromail may no longer use prisoners to process personal information.[8] Nevertheless, a general prohibition on inmate access to SSNs is appropriate, and California and Kentucky already have passed legislation to keep SSNs out of the hands of prisoners.[9]

Section 108 generally prohibits disclosure of the SSN in the private sector, subject to exceptions. We think it important to limit exceptions to the general prohibition in order to curb private sector use of the SSN. First, the exception for public health purposes should be limited to "emergency public health purposes." In its current articulation, this exception could allow medical providers and insurance companies to continue to rely upon the SSN in normal operations. Limiting the exception will encourage the industry to shift away from the identifier. We note that Empire Blue Cross is transitioning its 4.8 million customers away from the SSN as an identifier, demonstrating that it is possible for large health care operations to use an alternative identifier.[10]

Section 108 contains an exception for SSNs of the deceased, meaning that they could be freely traded on the market. We think there are important public policy reasons to place some protections on SSNs of the deceased. SSNs of deceased individuals should receive protection for the same reasons that justify protections for living individuals; those reasons include preventing fraud and identity theft. Additionally, criminals are known to assume the identities of deceased individuals in order to engage in criminal acts and to avoid law enforcement. Some protection for these identifiers is justified.

Section 109 codifies a much-needed protection for the SSN. Prior to the implementation of the Gramm-Leach-Bliley Act, CRAs and other entities sold SSNs in credit headers to individuals outside Fair Credit Reporting Act regulation. We understand that some businesses are still selling SSNs from credit headers that were collected before implementation of Gramm-Leach-Bliley. Section 108 would eliminate this unregulated sale of SSNs by tying the identifier to the credit report, and thus to protections in the Fair Credit Reporting Act.

Section 110 contains important protections against the practice of "coercive disclosure," a practice where an entity conditions provision of a product or service based on disclosure of the SSN. Maine, New Mexico, and Rhode Island have established

---

[7] *See* Ariz. Rev. Stat. § 28-3158; C.R.S. § 42-2-107; C.R.S. § 42-3-302; D.C. Code Ann. § 50-402; O.C.G.A. § 40-3-23; HRS § 286-109; HRS § 286-239; Idaho Code § 49-306; Idaho Code § 49-2444; Ky. Rev. Stat. Ann. § 186.412; Mont. Code Ann. § 61-5-111(2)(b); Nev. Rev. Stat. Ann. § 483.345; N.H. Rev. Stat. Ann. § 263:40-a; N.D. Cent. Code 39-06-14; Ohio Rev. Code Ann. § 4501.31; Okla. Stat. Ann. tit. 47, § 6-106 (2002); Pa. Cons. Stat. Ann. § 1510; Tenn Code Ann. § 55-50-331; Tex. Trans. § 521.044; Va. Code Ann. § 46.2-342; Wash. Rev. Code Ann. § 26.23.150.

[8] During litigation, Metromail claimed that they had not violated the woman's privacy, that they had no duty to inform individuals that prisoners were processing their personal data, and that the data processed was not highly intimate or embarrassing. *Beverly Dennis, et al. v. Metromail, et al.*, No. 96-04451, Travis County, Texas.

[9] Cal Pen Code § 4017.1, § 5071; Cal Wel & Inst Code § 219.5; Ky. Rev. Stat. Ann. § 131.191.

[10] *Empire Blue Cross Will End Use Of SSNs, Use Alternate Number System*, PRIVACY AND SECURITY LAW REPORT (Jun. 7, 2004) at 666.

protections against coercive disclosure, and we think it a good idea to federalize this important right to enhance privacy of the SSN.[11]

II. STATES HAVE INNOVATED CLEVER PROTECTIONS FOR THE SSN; CONGRESS SHOULD CONSIDER INCORPORATING THEM IN 108 H.R. 2971

In recent years, state legislatures have functioned in their traditional roles as "laboratories of democracy," creating new approaches to enhancing the privacy of SSNs. These privacy protections demonstrate that major government and private-sector entities can still operate in environments where disclosure and use of the SSN is limited. They also provide examples of protections that should be considered at the federal level.

Some States Have Placed Broad Prohibitions on Disclosure and Use by Government and Private Entities

Colorado Governor Bill Owens signed H.B. 1311, legislation that creates important new protections for the SSN that took effect this summer. The new law will limit the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state. The law requires the establishment of policies for safe destruction of documents containing the SSN. Insurance companies operating in the state must remove the SSN from consumers' identification cards. Finally, the legislation creates new penalties for individuals who use others' personal information to injure or defraud another person.

A law taking effect in January 2005 in Arizona prohibits the disclosure of the SSN to the general public, the printing of the identifier on government and private-sector identification cards, and establishes technical protection requirements for on-line transmission of SSNs.[12] The new law also prohibits printing the SSN on materials mailed to residents of Arizona. Exceptions to the new protections are limited—companies that wish to continue to use the SSN must do so continuously, must disclose the use of the SSN annually to consumers, and must afford consumers a right to opt-out of continued employment of the SSN. Arizona's new law is based on California Civil Code § 1798.85.

Special Protections Have Been Crafted for Students

A number of states have passed legislation limiting colleges and universities from employing the SSN as a student identifier. Limiting use of the SSN in this context reduces the risk of identity theft, as databases of student information, student identity cards, and even posting of grades sometimes contain SSNs.

In Arizona, major universities can no longer use the SSN as the student identifier.[13] In Colorado, as of July 2003, public and private postsecondary institutions were required to establish protections for the SSN and discontinue its use as the primary student identifier.[14] New York and West Virginia prohibit all public and private schools from using the SSN as a primary identifier.[15] Kentucky law allows students to opt-out of use of the SSN as student identifier.[16]

Protections Crafted for Public, Vital, and Death Records

Commercial data brokers obtain SSNs from a number of sources, including public records that individuals are required to file in order to enjoy important rights and privileges offered by society. For instance, marriage licenses have been a source for SSNs and a number of states, including Arizona, California, Indiana, Iowa, Kentucky, Louisiana, Maine, Montana, Ohio, and Michigan, have enacted legislative protections to prevent their disclosure.[17]

Birth and death records are rich in personal information, and states have acted to shield SSNs collected in these life events against disclosures. Arizona, California, Illinois, Kansas, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, New Hampshire, and other states limit the appearance of the parents' SSN on birth

[11] 2003 Me. ALS 512; N.M. Stat. Ann. § 57-12B-3; R.I. Gen Laws § 6-13-17.

[12] Ariz. Rev. Stat. § 44-1373.

[13] Ariz. Rev. Stat. § 15-1823. Rhode Island and Wisconsin have similar protections. R.I. Gen. Laws § 16-38-5.1; Wis. Stat. Ann. § 36.11(35).

[14] C.R.S. § 23-5-127.

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

[16] Ky. Rev. Stat. Ann. 156.160. *See also* Ky. Rev. Stat. Ann. 197.120.

[17] Ariz. Rev. Stat. § 25-121; Cal Fam Code § 2024.5; Burns Ind. Code Ann. § 31-11-4-4; Iowa Code § 595.4; Ky. Rev. Stat. Ann. 402.100; La. R.S. 9:224; 19-A M.R.S. § 651; MCL § 333.2813; Mont. Code Ann. § 40-1-107; Ohio Rev. Code Ann. § 3101.05.

records.[18] Similarly, several states restrict disclosure of the SSN in records associated with death.[19]

Protections Against Pretexting Should Be Considered

We wish to raise one additional concern here—even legitimate collection of the SSN contributes to unauthorized access to the identifier. That is, we are increasingly aware of manuals for private investigators and other materials suggesting that SSNs can be obtained from motor vehicle departments, applications for professional licenses, and even tax returns.[20] In these cases, the investigator probably obtains the identifier through a friend or contact working at the institution with a SSN. Alternatively, the manuals suggest the use of "pretexting," a practice where an investigator requests personal information from an entity while pretending to be another person or while pretending to have a legitimate reason for access to the information. The Gramm-Leach-Bliley Act prohibits pretexting with respect to financial, securities, and insurance companies, but the law doesn't apply to pretexting targeted at employers, utility companies, or other entities that have SSNs. The Subcommittee should consider whether expanding protections against pretexting would enhance the privacy of the SSN.

CONCLUSION

We think that the privacy and integrity of SSNs could be enhanced through the passage of federal legislation that limits the collection and approved uses of the identifier. We urge the Subcommittee to examine state laws that have created new, clever protections for the SSN. We look forward to continuing to work with the Subcommittee on this and other privacy matters.

Mr. STEARNS. I thank the gentleman.

I will start with my questions first.

Mr. Hoofnagle mentioned the possibility of an alternative to a Social Security number. Commissioner, do you think there is another way to do this instead of having Social Security numbers? That would obviate the need to show your Social Security number, and should Congress push that idea?

Mr. LEARY. My problem with this, Congressman, is if we were writing on a clean slate and starting all over again, I suppose you could imagine a system where there might be some other identifier. And going down the road, there may be other identifiers. I mean, there may be technology having to do with your eye, fingerprints or things like this, which will be much, much more secure identifiers than what we have today. That is down in the future. But we have, unfortunately, a system that has been in place for a long time that is very, very hard to turn around. Let me give you a purely personal example.

I first got my Social Security number when I turned 15 and had my first summer job. That was almost 60 years ago. In the interim, my Social Security number has been out there in innumerable employment records, employment applications, and records of various kinds. I agree with Mr. Hoofnagle that business has gathered these records reflexively for a long period of time. We were encouraged to carry our Social Security card around with us at all times to use as identification when I was young. Now, of course, they advise just

[18] *See* Ariz. Rev. Stat. § 36-322; Cal Health & Saf Code § 102425; 410 ILCS 535/11; K.S.A. § 65-2409a; 22 M.R.S. § 2761; Md. Ann. Code § 4-208; ALM GL ch. 111, § 24B; Minn. Stat. § 144.215; Miss. Code Ann. § 41-57-14; Mo. Rev. Stat. § 193.075; Mo. Rev. Stat. § 454.440; N.H. Rev. Stat. Ann. § 5-C:10.

[19] *See* Ariz. Rev. Stat. § 16-165; Cal Health & Saf Code § 102231; Idaho Code § 67-3007; Burns Ind. Code Ann. § 16-37-3-9; La R.S. § 23:1671; N.D. Cent. Code § 23-02.1-28.

[20] *See e.g.* Lee Lapin, HOW TO GET ANYTHING ON ANYBODY 533-543 (Intelligence Here, 3d ed. 2003) (section titled "How to Find Anyone's Social Security Number" suggests thirty sources for the SSN, including driver's license applications, bankruptcy filinga, court records, bank files, utility records, professional and recreational licenses, and employment files).

the opposite. We were encouraged to put the Social Security number on the envelope when we mailed in our tax returns. Now, of course, they tell us just the opposite. I suspect that someone who wanted to get hold of my Social Security number and who knew where to look could get it in about 3 minutes today. There is not much of anything that Congress can do about that.

All I am saying is that there is this embedded system, and whether there is an incremental value in attempting root and branch to change the way businesses do things is a very serious question.

Mr. STEARNS. Mr. Hoofnagle, when I have a credit report, my Social Security is part of that credit report; and I can get a copy of my credit report on the Internet for $35. Do you think that consumers should put their Social Security on the Internet?

Mr. HOOFNAGLE. That is a complex question. It can be transferred over the Internet if it is done in encrypted fashion.

Mr. STEARNS. If it is not encrypted, then—because you get these dialog boxes that say what you are sending is not protected.

Mr. HOOFNAGLE. If those cases, the consumers should never send their Social Security number. They do it over the phone, and the credit reporting agencies will make your credit report available by mail if you call, but consumers should only enter that information if it is encrypted.

Mr. STEARNS. I think it goes without saying, Equifax, Experian, TransUnion, these people are not necessarily—they have some legitimate arguments that they use this information to help the consumers and this bill, might, in fact, hurt the marketing or the dissemination of information that is valuable to the consumer. So would you understand their point of view? Do you think they have a legitimate problem—this is for all three of you—that these major data base collectors have some reservations about restriction, both application of civil and criminal penalties, because they might be liable for something they are doing just as a service to the consumer?

Mr. HOOFNAGLE. That is a legitimate concern, but I do think H.R. 2971 is a nuanced approach, and I think, going forward, Congress should have a nuanced approach that allows the use of Social Security numbers in some contexts but not in others.

We got a call from a consumer last week who was going to rent a refrigerator for her home. The company wanted her Social Security number to check her credit, but then they were going to use her Social Security number as her record identifier. So she would start receiving mail with her Social Security number in it. All the employees of that company would probably have her Social Security number. A nuanced approach would allow the transfer of the SSN to check the credit but not allow it for use as a customer identifier.

Ms. BOVBJERG. I like to put these things into three groups.

There are entities who have a legitimate need to use the Social Security number. With those, you want them to apply better protections; and I think that is something that you are looking at in this bill. You want entities who don't need the number to stop collecting it, another element of this bill. You want to protect sources like, for example, public records in the States and counties in par-

ticular where people may not know that their number is floating around and we have been told by the businesses involved are sources for them in getting personal information, which includes the Social Security number.

It is a nuanced approach that the entities who have a legitimate need, you want to allow them to continue to use it but protect it from being transferred to the wrong places, protect it from being displayed to people who don't need to see it.

When we have talked with businesses over the years that we have been doing this work about what would happen if you couldn't use the number, which would be I think a more Draconian approach than what we are discussing today, they felt that it would be—disruptive was the word they used. They would have to consider what they could find to track that would be both unique and that the person would keep for their lifetime that wouldn't change and something they might be able to exchange with other entities but that, ultimately, they would adjust.

Mr. STEARNS. Commissioner?

Mr. LEARY. I think we all agree that a nuanced approach is necessary. The question is whether or not some of the provisions in the bill are not nuanced. Let me pick one for example.

That is the notion that, somehow or other, a consumer can refuse to give a Social Security number to a business that requires it as a condition of doing business. Now you can understand why that right would make sense if, as Mr. Hoofnagle points out and I think rightly so, a lot of businesses have just gotten in the habit of using it as an identifier. But, it seems to me that that right of refusal would make no sense whatever if you are asking the business to extend credit to you or to give you merchandise on some kind of a payment plan where they need that Social Security number to access your credit history. If these businesses can't access your credit history readily, our financial system as we know it is going to be seriously impaired.

So writing a statute and then subsequently enacting regulations that distinguish between the legitimate request for Social Security number and one that goes too far is no easy task.

Mr. STEARNS. I am going to conclude, and I am going to say that the question would be then that the three large data base companies, in your opinions, should not fear this bill? Is that what the three of you are saying? You all agree with that? That Equifax, Experian and TransUnion, there is nothing in this bill that would make it difficult for them?

Mr. LEARY. There is some language in the bill that might even make it difficult for them, and I would like to submit something to the committee. Our written statement doesn't have a paragraph by paragraph analysis of the bill; and, with your indulgence, I would like to submit that.

Mr. STEARNS. You are saying you think the bill does have some reservations and you think it should be improved to better allow these people to communicate with consumers?

Mr. LEARY. Yes, sir.

Mr. STEARNS. Ms. Bovbjerg, is your opinion the same? Just yes or no. These people are the big players here, and I want to see if you think the bill would work for them or not.

Ms. BOVBJERG. What we have heard out in the business world is that it is not impossible to do business without the Social Security number. But if use of the Social Security number were restructured, there could be a period of disruption, and there could be a period where people don't get the services that they have become accustomed to.

Mr. STEARNS. You are saying the bill as it stands right now in your opinion would not affect these three companies?

Ms. BOVBJERG. I can't answer that question.

Mr. STEARNS. This is a subjective opinion. The Commissioner is saying, yes, I think it could, but some parts of it should be changed. Should some of this be changed, you are an expert here, so these folks can communicate with the consumers or not?

Ms. BOVBJERG. I can't say from their perspective. I don't have the information to do that. I can say that I think the bill would go a long way toward filling in the gaps.

Mr. HOOFNAGLE. I wish to echo those comments. I cannot evaluate it from the perspective of the credit reporting agencies. But I would point out major companies like Blue Cross and Blue Shield of New York have switched away from the Social Security number. That is a company with 4.8 million subscribers.

Mr. STEARNS. Seems you could use the license number on your driving permit would be a possibility or just eliminate the Social Security except for the last four digits and use that as a tool, except in very select cases.

My time is expired and, with that, the ranking member.

Ms. SCHAKOWSKY. Mr. Hoofnagle, I am—I bank on-line, and my password is my Social Security number. Are you saying that there is danger in that? And also that there is not any particular good reason for that to be my PIN number to log in? Actually, they give a PIN number, but my first identifier, though, is my Social Security number.

Mr. HOOFNAGLE. It is not a good idea to use the Social Security number as the main identifier for your account. It is not necessary for the company to do so. The general problem is that your Social Security number might be available in other contexts. It might be in public records. It might be in the business records of companies without good security, and access to the number could provide someone an opportunity to interfere with your accounts.

Ms. SCHAKOWSKY. Does that mean each time I call for help, the help line, that the individual who is looking at my account is also looking at that screen that has my Social Security number and has complete access to that?

Mr. HOOFNAGLE. It depends on the company. Some companies have layered access to personal information and essentially condition access on the need for it. Some companies do not. So it is entirely up to whether or not the company has good internal security protocols.

But the risk you are articulating here is the primary identity theft risk, and there is very little consumers can do about identity theft because so much of the crime that occurs is a result of insider access.

Ms. SCHAKOWSKY. This is a financial institution. This isn't a small bank. What is the indication of encryption or other security? How do I know that the number I give is encrypted?

Mr. HOOFNAGLE. Consumers have very little insight into security practices. One of the core ideas behind privacy is so-called fair information practices. It is the idea that you have access to your personal information, that you can audit access to your information and that there is real security safeguards.

Ms. SCHAKOWSKY. Is there an icon or anything that tells me? Normally, I never looked for that, and I have never noticed it. Is there something that says it is encrypted in some way?

Mr. HOOFNAGLE. In a standard browser, a little lock icon should appear at the bottom of the browser. But the consumer, in addition to seeing that little lock, should click on the lock to make sure that the certificate that is being issued by the Web site matches the bank's Web address. That extra step of matching the certificate is beyond most consumers.

Ms. SCHAKOWSKY. The issue of restitution for consumers seems to be one that has not been particularly addressed. I know that, in looking through your testimony, Mr. Leary, that you get a lot of complaints and those are shared, I guess, with law enforcement. But what we hear in terms of constituent complaints is that it is just a hassle beyond tolerance to try and get any restitution or relief or even getting it corrected, much less even getting—I wonder if any of you could comment on that and what kinds of things we could be doing to help once the theft has already occurred.

Mr. LEARY. Well, there is an irony here, too, as well. As you know, the Federal Trade Commission does administer some restitution programs and in a very limited way. And by that, I don't mean that our remedies are limited, but our resources are limited. So our efforts are necessarily selective, exemplary and usually aimed at covering as large a group of consumers as we can in a particular complaint against a particular company. In other words, we are not equipped to deal with the individual constituent complaints that you have and which I know are a serious problem.

One of the great ironies here, in the world we live in today, is that Social Security numbers are a very quick and ready way to find people who might otherwise not be able to be located for the purpose of administering redress programs to wide numbers of people who have been injured. I wish I could tell you that there is some way that we, the Federal Trade Commission, can help you with these individual consumer complaints, but I am afraid that we have to deal only with things that have a much larger impact.

I get consumer complaints mailed in to me as well, and one of the sad and frustrating things is that we simply don't have the resources to deal with these individual things. We can give people advice. We have advice in the booklets as to whom you can go, steps you can take to repair your credit, at least to cutoff the damage. But when it comes to actually getting redress from the wrongdoers, that is a real tough job.

Ms. BOVBJERG. I don't have a lot to say about redress, but I did want to say that I think things have been getting a little better with regard to law enforcement coordination and that does help people. But it is very frustrating and disheartening for individuals

where the crime doesn't meet a threshold that a Federal law enforcement agency will investigate. The victims have to go to State and local enforcement, and the coordination may or may not be there, depending on where the crime occurred, and where the person lives. It is terribly frustrating for them, and you can understand why they would like restitution, but, even then, I don't know that it can compensate for their time, and for the damage that such a crime has done to this person's life.

Mr. HOOFNAGLE. A number of victims have attempted to sue companies that have improperly granted credit to imposters, and those lawsuits have generally failed, unfortunately from our view. We think a great protection moving forward would be the ability of a victim to actually pursue a credit-issuing bank or credit-issuing retailer that negligently extends credit to an imposter. There are amazing examples of this behavior where an imposter applies for credit and only the Social Security number matches and nothing else matches and the creditor still issues the account, and we think that needs to be reined in.

Ms. SCHAKOWSKY. There are legal impediments to pursuing that in the courts.

Mr. HOOFNAGLE. There are four cases that have been litigated in the Federal Courts on that issue, and all four have failed. The most recent was before the Supreme Court of South Carolina, where that court said that there was no duty between the credit issuer and the victim. So even though the credit was granted in the victim's name to an imposter, the court still would not recognize a right of action.

Mr. STEARNS. The chairman of the full committee, Chairman Barton.

Chairman BARTON. I don't have too many questions. I want to thank you for holding the hearing and thank our panelists for being here.

My question goes to the heart of this whole issue. Social Security numbers were really not created to be a surrogate for a national identification number. They were created to help track people who were paying taxes into the Social Security Trust Fund, Old Age Survivor and Independent Beneficiary Fund, and to pay the benefits out. But they have become a surrogate national identity number.

I took out a loan to buy a new home this past year, and I had to give my Social Security number. I opened a bank account when I got married. It wasn't an option. You want to take this loan out, you give us your Social Security number. You want to take this loan out, you give us your Social Security number.

My first question is, should we just begin to assume that the Social Security number is a national identity number and proceed forward or should we continue under this charade that it is really not a national identification number?

Mr. LEARY. I will start, Mr. Chairman.

We had a brief discussion of that shortly before you arrived, and I agree with you it has evolved in a way that probably people didn't foresee 65 years ago. But it has, as a practical matter, now become the basis on which credit decisions are made. It has been a very important way of identifying who someone named John Jones is,

and distinguishing that person from some other John Jones who has a terrible credit history.

One of the reasons that you and I are able to walk into a store in a strange town where nobody knows us and walk away with fairly expensive merchandise is because there is a recognized identifier. So that is the system we have. Now there can be—and I hope someday going down the road, long term, there will be—much more highly technical ways of ensuring that you are who you say you are, but for the moment this is what we are stuck with.

Mr. Hoofnagle made a very good point, though, and that is there are some businesses that are very careless, and they assume that if you have the Social Security identifier they can take it as a given that you are who you say you are, notwithstanding the fact that a lot of other things don't match. We are working on ways, by the way, to see if we can't make some affirmative suggestions in that regard for more positive supplements to that kind of an identifier.

Ms. BOVBJERG. Chairman Barton, I am Barbara Bovbjerg, From GAO, and I do a lot of work with the Social Security Administration. I know SSA would be completely horrified at the prospect of using the Social Security number as a national identifier. They would then be responsible for enumerating everyone, not just the people who are born American citizens, not just the people who are authorized to work, but everyone. And perhaps arguably that might make their task easier, as they might not have to sort through people. But it would change the whole nature of the Social Security number and its relationship to the Social Security program.

In thinking about that, one can argue that today it is a de facto national identifier, but I think that if it is our national identifier, we are not really protecting it very well, and that if it were to be a national identifier, we would have to do things very, very differently than we do now.

Chairman BARTON. We have to go—to quote a poker term, we either withdraw or go all in. We are kind of half invested in the pot right now, and we haven't committed to it. As we become technologically advanced, we need to have a debate and decide, either you continue to use this and protect it or back away and come up with a real national identification number. That is what it is.

And Mr.—the first gentleman's point—I am a frequent flyer. Under this test program, they have my thumbprint and eye print. I walk up to National Airport or Reagan Airport, and the line is 300 people long. I go up and look in this little thing; and it says, that is Joe Barton, and he can go through.

So, I mean, the technology is there if we wanted to use it. And so that is really the question at this hearing, what do we want to do.

Mr. STEARNS. Would the gentleman yield?

Chairman BARTON. Sure.

Mr. STEARNS. How do the rest of us get that service?

Chairman BARTON. You just have to sign up for the program.

Mr. STEARNS. Just with the airlines itself?

Chairman BARTON. Yeah. I am sure Mr. Green is signed up.

Mr. GREEN. Mr. Chairman, if the gentleman would yield, I signed up, but since I use Continental Airlines that service is only

good for American Airlines out of Reagan. But hopefully we will get some type of seamless system.

Chairman BARTON. And that is my point. It took me about 5 minutes to go through. I don't think they asked for my Social Security number when I signed up. They just asked for my driver's license, and then they took my thumb print and my eye print and that was it.

Mr. Hoofnagle, do you want to——

Mr. HOOFNAGLE. Thank you, Chairman Barton. We are concerned about the expanding use of the Social Security number. But I did want to remark that people frequently, when thinking about privacy, say that the toothpaste is out of the tube and you can't put it back in.

But I don't think that is the case. And the best evidence of that is the telemarketing Do Not Call list that the Federal Trade Commission created with the Federal Communications Commission and by this Congress. And I think that is a compelling example of where we can take privacy back and we can establish safeguards.

And the whole history of privacy law has followed the same model, where people have said it is too late, the information is already out there, but we have passed legislation to protect personal information and it protects us from that point forward.

Gramm-Leach-Bliley, too, protects Social Security numbers in important ways. And it might not protect you and me, but it will protect our children. So I think, going forward, we should be optimistic.

Chairman BARTON. I am for that.

You know, the conservatives—when we come to Congress, the conservative mantra is, no national identification number. You know, we don't want big brother to know all there is to know about us. But, de facto, if you use the modern industrial banking and credit system, you are going to have to give your Social Security number.

And you have to have it. I don't think you can refuse to have a Social Security number. I think you have to have one. If you work, I think you have to have one. I don't think I could say, I don't want one, I am not going to pay Social Security taxes; or I am going to pay Social Security taxes, but I don't want a number. I think whether you get one or not, you get it.

So I think we ought to have the debate and decide how to protect the Social Security number, and then decide what we want to do about the national ID number.

With that, Mr. Chairman, I am going to yield back the 3 minutes that I have overused.

Mr. STEARNS. I thank the gentleman.

The gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman. And I know, as our chairman of the full committee mentioned, a lot of us have concern about use of our Social Security numbers; and I think we do have a de facto ID number.

Now, I understand when I go and apply for a loan, a home loan, they want my Social Security number because sometime along the way I am going to deduct that interest on that loan and so that mortgage company is going to report that not only to myself, but

I assume to the IRS. There are reasons that we have a Social Security number for tax purposes.

But I also know when I asked to rent a U-Haul truck, they wanted my Social Security number. And I refused. I still got the truck. I don't know how often that would happen—simply because they want to check your credit rating, and I know that is our identifier.

I guess my concern, and I appreciate our panel and the hearing, Mr. Chairman, is because of the three major credit bureaus we have; and I know under current law they are required to exchange the information. If I, for example, lost my credit cards, or I felt they were stolen, I would notify one, and all of them would be, the other two would be notified.

But I do share the concern. In fact, I—being from Texas, I have some concern because when I did the American Airlines—even though I am not a frequent flier with American, it is Continental—they did ask for my driver's license number. But I always understood that someone can go to my driver's license number in Texas, it is on the Web, and find out all my information, probably including my Social Security number.

Is that correct, that States will provide that information, and they don't—State governments really don't guard the information, particularly a Social Security number?

Mr. HOOFNAGLE. Representative Green, since 1998 the Driver's Privacy and Protection has set in, opt-in, meaning affirmative consent protections for your information at the motor vehicle association. The problem is that not all States have implemented the Driver's Privacy and Protection Act. Florida, for instance, failed to implement it, and they will not come into compliance with the law until October 1 of this year. And, as a result, there is a lot of information out there that is not available in other States. But Federal law should protect that data.

Mr. GREEN. Well, I would be interested if you could provide to the committee other States, other than Florida, that maybe are not in compliance with the law from 1998.

Mr. HOOFNAGLE. I would be happy to do so.

Mr. GREEN. One of the other concerns is, when credit bureaus flag reports once there is fraudulent activity, is there a specific time by which credit bureaus must respond to continue to flag that particular account? Because I know oftentimes with stolen identities, it may not happen within 30 days or 6 months, but can happen later. Is there any kind of timeframe that you know of that most of the credit reporting agencies have?

Mr. LEARY. I can't answer that question, Congressman. We will get an answer for you.

I will just tell you a personal experience. I lost a driver's license about 2 years ago, and reported it, simply out of an excess of caution, to the credit agencies. And 2 years later, they still have a flag on my accounts, and it is extremely difficult to this day for me to get a new line of credit or something like that. They ask for all kinds of additional information. And I am glad to provide it under the circumstances because I feel safer.

Mr. GREEN. And I agree. That is why I would rather those flags not drop off, because once that number is available on that, the

folks who want to use it for illegal purposes, it could used again 30 days or 6 months or, like you said, maybe even a year later.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman.

As customary, when we have completed the members of the subcommittee, we certainly welcome the opportunity for others to participate. And we are fortunate to have the author of the bill, Congressman Shaw. So he has been kind enough to come here, and I welcome his comments and anything he would like to put in the record.

Mr. SHAW. Thank you, Mr. Chairman. And I do have a statement that I would ask unanimous consent to be placed in the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. SHAW. And just to make a few observations—and I shall not take the full 5 minutes—in listening to the questioning from the members and, of course, the replies from the panel of witnesses, many of whom have appeared before my Social Security Subcommittee, I think you are getting the full thrust of what we are doing and what we are trying to accomplish.

Clearly, the Social Security number was never, never intended to be an identifier, it never was. We need to do a lot to protect this number. This particular portion of the bill that this committee has jurisdiction over is of particular importance because it stops the widespread use—or requirement for the wide spread use—of Social Security numbers just simply to open accounts and just simply to do business with particular individuals.

You will find that the utilities ask for it, the phone company asks for it. If you go try to open an account at a video store, the chances are they are going to want it. Opening up credit at a department store, at Burdines Department Store in Florida, which is part of the Burdines-Macy's group, they had, I recall, a sale where you get 20 percent off, and I was buying my wife's Christmas present—20 percent off if I would open an account. And I said, Well, that is a good idea, and I offered to open the account. And the first thing they wanted to know is my Social Security number; and I ended up having to pay 20 percent more because I wasn't going to give it, and they weren't about to give me credit.

But these are very important things. The use of it as a serial number in the military is of great concern. We have had testimony before our committee of the tremendous problems that people go through and the problems that they have once their credit has been stolen, once their identity has been stolen. And the Social Security number is the key to it.

There is actual commerce in Social Security numbers that is going on quite legally in this country. I think if you are computer literate, you can probably go to a computer and find my Social Security number.

That is not right. We need to stop this practice. We need to stop the wide spread use of Social Security numbers for things that they were never intended for. That Social Security number is the property of the government and the person to whom it was issued, period, and it shouldn't be used for any other purposes other than governmental purposes.

We must address the openness of documents, government documents, because you can go to court files and find the Social Security number.

These things have to be dealt with. And again, Mr. Chairman, I applaud you for moving this legislation forward. I am hopeful that we can get this bill. If we can't in the few days left in this particular session, maybe we can come back and use this as the groundwork necessary to speed this bill through. We need this particular portion of it to stop the spread of this crime.

And with that, I yield back, Mr. Chairman.

[The prepared statement of E. Clay Shaw, Jr. follows:]

PREPARED STATEMENT OF HON. E. CLAY SHAW, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Social Security numbers, also known as SSNs, are integral to Americans' everyday lives. The government requires us to have an SSN for employment, paying taxes, and numerous other transactions. And even though it is not required by law, many businesses ask for individual's SSNs to provide goods and services.

Because the SSN is involved in so many transactions and is the key to our personal and financial information, it is one of the pieces of personal information most desired by identity thieves, and plays a pivotal role in identity theft. That is why I applaud the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection for holding this important hearing. Congress must act to help consumers protect their SSNs, which is a vital step toward identity theft prevention.

Identity theft is a vast and growing problem. Overall, nearly 10 million people—or 4.6 percent of the adult population—discovered that they were victims of some form of identity theft in the year prior to a 2003 Federal Trade Commission-sponsored survey. The crime resulted in nearly $48 billion in losses to businesses, nearly $5 billion in losses to individual victims, and almost 300 million hours spent by victims trying to resolve their problems.

Although Congress has enacted laws in recent years, such as the "Gramm-Leach-Bliley Act" (P.L. 106-102), and the "Fair and Accurate Credit Transactions Act of 2003" (P.L. 108-159) to help protect personal information and prevent identity theft, we do not yet have a law that provides broad-based and consistent protection for SSNs, especially regarding its collection and use in the private sector.

To close the gap in SSN privacy protection identified through reports by the Government Accountability Office, testimony, and other research, I introduced the "Social Security Number Privacy and Identity Theft Prevention Act of 2003" (H.R. 2971). This bipartisan bill, which was unanimously approved by the Committee on Ways and Means on July 21, 2004, would restrict the sale and public display of SSNs, close an existing credit header loophole that allows widespread dissemination of SSNs, tighten procedures for issuing new SSNs, and establish penalties for violations. H.R. 2971 has been referred to the Committee on Energy and Commerce to consider a provision that makes it more difficult for businesses to deny services if a customer refuses to provide his or her SSN.

Providing for uses of SSNs that benefit the public, while protecting these numbers from being used by criminals, or even terrorists, is a complex balancing act. While there are powerful consumer benefits from business use of SSNs as a common identifier, the Committee on Ways and Means Subcommittee on Social Security, which I chair, has heard testimony on how identity theft rings may use an employee of a business to obtain names, SSNs, and other personal information in large batches.

For this reason, the Federal Trade Commission and others advise Americans to avoid giving out their SSN unless it is absolutely necessary, and my bill puts that advice into law. Consumers should have the option to refuse providing their SSNs without being denied goods and services, unless the SSN is required by law. While necessary uses of SSNs must be, and are preserved in my legislation, widespread collection and use of SSNs simply for convenience's sake must stop in order stem the growing tide of identity theft.

Again, I thank the Committee for holding this hearing and look forward to working with my colleagues to act quickly to help protect SSN privacy and prevent identity theft.

Mr. STEARNS. I thank my colleague, and I appreciate his attendance here. I think it has helped our hearing. We have finished our questions. I would conclude by saying that, as Mr. Shaw mentioned, the Ways and Means Committee had a hearing, marked it up. So we try to encourage our committee to look at this bill and look at it carefully. And perhaps, Commissioner, if you have any changes or suggestions you think should be done on the bill, as you alluded to, we would like to see those.

All of us know that the Fair Credit Reporting Act had an amendment so that when I go to a restaurant now, I don't get a full MasterCard number back; they truncate it, so I only get the last four numbers. And that was a great step forward.

And so these are the types of things, if you move incrementally, you get improvements that will help out to protect people's identity.

So anything we can do—I think, based upon the facts that I gave in my opening statement, with as much as $5 billion a year lost to individuals and $48 billion a year lost to businesses—which is really the Federal Trade Commission's statistic—this is a formidable problem; and certainly we can't let this continue.

And as also pointed out, I think, by the committee and the witnesses, this is on the rise, too, so that this is something that we should work for and look for solutions.

With that, the subcommittee is adjourned.

[Whereupon, at 3:15 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF ACA INTERNATIONAL

SOCIAL SECURITY NUMBER PRIVACY AND IDENTITY THEFT PREVENTION ACT (H.R. 2971)

ACA International (ACA), on behalf of the credit and collection industry, strongly opposes the Social Security Number Privacy and Identity Theft Prevention Act (H.R. 2971), which would undermine the practices voluntarily instituted by private industry, many of which have subsequently been required by federal law, to protect the privacy of consumers' personal identifying information.

RATIONALE

ACA shares Congress' concern about the increase in the incidence of identity theft. We applaud legislative proposals that would serve to deter identity thieves and levy harsh punishment against those who obtain or use personal identifying information for an unlawful or illegal purpose. However, these well-intentioned efforts should not pose an unreasonable burden upon businesses which must use Social Security numbers (SSNs) to positively identify a particular person. Therefore, ACA must oppose H.R. 2971, as currently drafted, as it does not specify that the purchase, sale or display of an individual's SSN for purposes of enforcing a credit obligation or collecting a debt would be legal should H.R. 2971 become law.

Furthermore, as the legislation would provide broad powers to the federal government for access, use and display of an individual's SSN, ACA is concerned that H.R. 2971 would not make adequate remedy available to an individual whose identity is stolen through the negligent actions of a government agency. Unlike other statutes, in which a private cause of action can be brought by an individual whose identity is stolen, and credit history and consumer credit report damaged, the doctrine of governmental immunity would likely prevent such recourse to an aggrieved individual under H.R. 2971.

PROTECTIONS ALREADY IN PLACE

As the nation's premier trade association representing credit and collection professionals, ACA places great emphasis upon the education of its members, to encourage the highest standards of business ethics and full compliance with the myriad of federal and state laws that currently govern the industry. Many of these laws mandate

specific requirements to protect the security and privacy of consumers' personal information, including their SSN.

ACA's creditor and collector members are subject to the Fair Debt Collection Practices Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, the Truth-in-Lending Act, the Health Insurance Portability and Accountability Act and the Fair Credit Reporting Act recently reauthorized by the Fair and Accurate Credit Transactions (FACT) Act, which all contain provisions related to consumer privacy. The FACT Act included several new safeguards to combat identify theft. The Federal Trade Commission is currently writing regulations to carry out the significant legislative requirements of the FACT Act related to new duties for data furnishers and others to prevent and fight identify theft.

Layered with these federal requirements are state laws that govern the practices of creditors and third-party collectors and address consumer privacy protections. H.R. 2971's sweeping provisions could prohibit businesses in the consumer credit and collection industries, which are vital to our nation's economy, from obtaining and using SSNs to accurately locate consumers and collect owed child support, and other important financial obligations.

PROPOSED AMENDMENT TO H.R. 2971

To be clear, ACA opposes the passage of H.R. 2971. However, if the bill does move forward in the legislative process, we respectfully submit the following amendment to address the concerns of the credit and collection industry. ACA proposes that language similar to that which currently exists under the Fair Credit Reporting Act be added to H.R. 2971, clarifying that the sale, purchase, or display of an individual's Social Security account would be permissible for purposes of enforcing a credit obligation.

Specifically, under the title "Prohibition of the Sale, Purchase, or Display to the General Public of the Social Security Account Number in the Private Sector" in Section 208 (c) Exceptions, ACA would propose that another exception be added as follows:

"(H) to the extent necessary in the enforcement of a credit obligation or the collection of a debt."

CONCLUSION

As credit and collection professionals, ACA members take the responsibility of safeguarding the security of sensitive consumer data, including SSNs very seriously. The member companies of ACA, representing over 100,000 credit and collection employees nationwide, comply with the existing framework of federal and state laws designed to protect consumers. ACA commends Congress for leading the fight against identity theft. The FACT Act passed last year and the recently passed Identity Theft Penalty Enhancement Act (H.R. 1731) were well-designed pieces of legislation intended to provide real relief for ID theft victims and deter would-be criminals. H.R. 2971, however, is a misguided and unnecessary bill that will do more harm than good.

ACA INTERNATIONAL

ACA International, formerly known as the American Collectors Association, is the association of credit and collection professionals. Founded in 1939, ACA International has approximately 5,300 members, including third-party collection agencies, attorneys, credit grantors and vendor affiliates. Headquartered in Minneapolis, ACA International serves members in the United States, Canada and 58 other countries worldwide. For more information on ACA International visit http://www.acainternational.org.

PREPARED STATEMENT OF FINANCIAL SERVICES COORDINATING COUNCIL

This Statement for the Record is being submitted on behalf of the Financial Services Coordinating Council—or "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 country, 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 on the use and misuse of social security numbers (or "SSNs"). Our

comments focus on the integral role of social security numbers in United States commerce; the many consumer benefits that result from financial institutions' use of these numbers; 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 social security numbers, 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.

We would urge the subcommittee to exercise caution in its deliberations on any legislation in this area, including consideration of H.R. 2971, the "Social Security Number Privacy and Identity Theft Prevention Act of 2004", given the significant unintended consequences that such legislation could engender.

Our testimony today makes three fundamental points:

- *First,* following the lead of the U.S. Government for the last 65 years, businesses' legitimate use of social security numbers as unique identifiers of individuals is now woven into the fabric of commercial transactions throughout the country. The use of these numbers 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 social security numbers 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 transactions.
- *Third,* Congress has recently enacted comprehensive privacy protections under the Gramm-Leach-Bliley Act that, among other things, place stringent restrictions on financial institutions' use and transfer of social security numbers. In light of these provisions, the FSCC strongly believes that further legislative restrictions on financial institutions' use and transfer of social security numbers are unnecessary.

Our statement also discusses the potentially negative impact of social security number restrictions on financial institutions' legitimate use of public records.

FSCC POSITION ON H.R. 2971

As a preliminary matter, the FSCC would like to express its serious concerns with H.R. 2917 as adopted by the House Ways & Means Committee. At its core, the legislation seeks to restrict the availability of social security numbers to the general public. It does so by limiting the sale, purchase and display of such numbers. It imposes limits on the ability of commercial entities to collect these numbers when offering a product or service. It also imposes unclear limits on disclosures of social security numbers to government agencies and the maintenance of social security numbers in ordinary business records. Unfortunately, we believe that the bill may have the unintended consequence of restricting a wide variety of legitimate business activities that pose no danger of the public display of social security numbers. Ironically, we remain concerned that H.R. 2971 will have the effect of actually *limiting* our ability to combat identity theft and fraud, and to otherwise serve our customers. It is our collective associations' view that, with respect to financial institutions, existing law already provides consumers with significant protections regarding the misuse of social security numbers, making additional restrictions unnecessary and potentially counterproductive.

As the Subcommittee is aware, in 1999 Congress enacted historic privacy protections as part of the Gramm-Leach-Bliley Act (GLBA). The GLBA subjects the financial services industry to a comprehensive privacy framework that requires annual disclosure of the company's privacy policies, allows customers to direct the company 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 and confidentiality of nonpublic personal information. *Importantly, under GLBA, social security numbers 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, Congress just last year enacted comprehensive legislation addressing concerns over identity theft as part of its passage of the "Fair and Accurate Credit Transactions Act of 2003 (FACT Act)". Taken together, 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.

The proposed bill, however, would create an entirely new regulatory structure for social security numbers and add it on top of a GLBA structure. For example, financial services companies regularly sell, for a price, assets between themselves and with secondary market institutions (e.g., home mortgages), such assets having social security numbers embedded in the files. Technically, these would be "sales" prohibited under the bill. (These would unlikely be a "trade or business" sale exempted under the bill). In addition, institutions regularly transfer information within their corporate families, either through central databases or otherwise, often in exchange for some compensation. Again, this could be prohibited under the proposed bill, notwithstanding the fact that such transfers of information help financial institutions efficiently service customer accounts. Moreover, financial institutions regularly use third party databases that purchase data from public databases and other sources that institutions check against to uncover fraud, identity theft and credit risk. These data compilers are not "consumer reporting agencies" under the Fair Credit Reporting Act (FCRA), and thus would be subject to the bill's limitations on purchase and sale. Ironically, each of these legitimate transfers of information benefit consumers and often facilitate our members' ability to better serve customers needs, combat fraud and root out identity theft, yet could be restricted under the bill. These are just some examples of legitimate, customer-beneficial activities that are called into question. There are undoubtedly others.

The bill does provide the Attorney General of the United States with the ability to exempt other transactions from these prohibitions. As a practical matter, the AG is not familiar with the operations of financial institutions and would be ill-suited to craft appropriate exceptions that protect legitimate business activities. The Justice Department would certainly not be able to respond quickly to questions that would arise over the implementation of this exception. Moreover, delegating that authority to financial services regulators (as the bill permits), while potentially helpful, creates a great deal of regulatory uncertainty, inserting levels of regulatory bureaucracy in an area already adequately dealt with under federal law. As noted before, GLBA already establishes broad restrictions on the disclosure of nonpublic personal information, while specifically enumerating focused exemptions for legitimate business activities. Congress vigorously debated these GLBA rules and exemptions, which various State and Federal regulators have since implemented after extensive notice and comment periods (e.g., Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Federal Trade Commission, Securities and Exchange Commission, and state insurance commissioners have all engaged in such reviews). Further action in this area, as it applies to financial institutions, is not necessary.

As a practical matter, we do not believe that the financial services community is really the subject of the concern that this legislation is attempting to combat. We use social security numbers, 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 these numbers accessible to the general public. As a result, we believe that this 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 social security numbers play in U.S. commercial activities.

As the GAO noted in its February 1999 report,[1] the Social Security Administration created social security numbers 65 years ago 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. 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. More-

[1] "Social Security—Government and Commercial Use of the Social Security Number is Widespread," February 1999, GAO/HEHS-99-28.

[2] *Id.* at p.4.

over, 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 not only complied with federal requirements to use SSNs as identifiers for federal laws unrelated to social security, such as income tax reporting. 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 as a unique identifier 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 report for a given individual. And as set forth in considerably more detail in Attachment A to this testimony, the banking, insurance, and securities industries each use SSNs as unique identifiers for a variety of important regulatory and business transactions, primarily to ensure that the person with whom a financial institution is dealing really is that person. Set forth below is a very incomplete sample of the many financial institution uses of SSNs that are listed in Attachment A:

- To combat fraud and identity theft;
- To accurately assess underwriting risk;
- To assist in internal benefits tracking;
- To identify money laundering activities;
- To comply with securities law reporting requirements;
- To transfer assets and accounts to third parties;
- To comply with "deadbeat dad" laws;
- To verify appropriate Department of Motor Vehicle records when underwriting auto insurance;
- To obtain verifiable medical information to underwrite life, disability income, and long term care insurance;
- To locate policyholders to pay insurance proceeds;
- To facilitate a multitude of administrative functions.

As noted in the GAO report, "[s]imply stated, 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] Put another way, the use of SSNs as common unique identifiers is now woven into the very fabric of both governmental 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, including those financial institution uses listed in Attachment A, in the forefront when considering proposals to restrict the use of SSNs.

UNINTENDED CONSEQUENCES OF BROAD RESTRICTIONS ON USE OF SOCIAL SECURITY NUMBERS

As a result of the widespread use of social security numbers for legitimate purposes, the FSCC remains fundamentally concerned about the unintended consequences of legislation that is intended to restrict the abuse of these numbers. Failure to carefully target legislation to avoid these unintended consequences risks serious harm to consumers and the smooth operation of the U.S. economy. Let me provide some specific examples:

- *Potential Harm to Consumers.* Financial institutions' use of social security numbers makes it possible for them to provide a level of service to customers that would otherwise not be possible. By using such numbers to verify individual identities, credit bureaus and others can quickly provide financial institutions

[3] *Id.*
[4] *Id.*, p.2.

with accurate credit histories and verification information on people seeking loans, insurance, securities, and other financial products. This in turn permits a financial institution to act swiftly and efficiently on applications or requests related to these products. Use of social security numbers also enables financial institutions to provide more seamless administrative service, e.g., by allowing a life insurer to more easily verify the identity of an individual seeking to change a beneficiary under a life insurance policy. The FSCC's concern is that a broad restriction on the sale or use of social security numbers, however 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.* Social security numbers are critical for fraud detection. Banks, insurance companies, and securities firms rely on information available from both public and private sources—with embedded social security numbers 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 make sound underwriting decisions that minimize losses. The sophisticated processes used for these purposes rely fundamentally on social security numbers as the common unique identifier to assemble accurate and verifiable information for a given individual. Put another way, without a unique common identifier such as a social security number, 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 social security numbers 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 social security numbers 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 social security numbers as the basis for account identification. When it sells such an asset, a financial institution could be viewed as technically "selling" the embedded social security number as well. Thus, legislative efforts that "directly or indirectly" limit the transfer of social security numbers 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.

THE PROTECTIONS OF THE GRAMM-LEACH-BLILEY ACT

The FSCC believes there is no need to further restrict the use of social security numbers by *financial institutions* in light of the strong social security number restrictions that apply to such institutions under the Gramm-Leach-Bliley Act ("GLB Act"). The GLB Act and its implementing regulations treat a financial institution consumer's social security number as protected "nonpublic personal information."[6] As a result, each financial institution consumer has the right to block a financial institution from selling or transferring his or her social security number to a non-affiliated third party or the general public.

There are exceptions to this general rule for legitimate transfers of social security numbers, such as ones that are necessary to carry out a transaction requested by the consumer; to protect against fraud; to provide necessary identifying information to a credit bureaus, etc. *However, even with respect to such legitimate transfers of social security numbers, 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.* Indeed, this unprecedented restriction on the re-use and re-disclosure of consumer information, including social security numbers, was recently upheld by the federal district court of the District of Columbia.[7]

---

[5] Existing law already includes provisions that prohibit identity theft. Stealing someone's identity is punishable by civil and criminal penalties under 18 U.S.C. 1028. Moreover, the Gramm-Leach-Bliley Act bans pretext calling, which is a basic tool of identity thieves.

[6] *See, e.g.*, 12 C.F.R. § 40.3(o), generally defining 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' (emphasis added).

[7] *ISRG v. FTC*, C.A. No.: 00-1828 (ESH) (Dist. DC, April 30, 2001).

In short, as the result of the GLB Act's carefully-targeted restrictions, a financial institution consumer is fully protected with respect to a financial institution's transfer of social security numbers, yet legitimate and important uses of these numbers remain permissible. In light of these restrictions, no additional restrictions on use of SSNs by financial institutions are warranted.

CONCERNS OVER RESTRICTIONS ON ACCESS TO PUBLIC RECORDS

Finally, some concerns have also been expressed regarding the inappropriate use of social security numbers 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 such 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 such 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 court bankruptcy records; public records involving liens on real estate; criminal records and fraud detection databases; and similar types of public records. Financial institutions also indirectly use such records for the same purposes by relying on databases developed by 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 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.

Finally, even if financial institutions were exempted from restrictions on access to public records containing social security numbers, such restrictions could still create indirect problems for financial institutions and their customers. For example, if a social security number were stricken from a public record, it is possible that the ability to use that record for legitimate purposes would become impossible because of the expense involved in verifying the identity of the person covered by that record. The consequences could be 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 social security numbers in their internal nonpublic 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 social security numbers 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 GLB Act's restrictions on financial institution disclosure of social security numbers, we believe that no new SSN restrictions are required for the financial services industry.

ATTACHMENT A

ACTIVITIES POTENTIALLY IMPAIRED BY RESTRICTIONS ON SOCIAL SECURITY NUMBERS

As noted above, a wide range of legitimate activities conducted by financial institutions would be affected by broad restrictions on the use of social security numbers. Set forth below are examples of such activities, grouped by the respective industries represented by the FSCC.

I. Banking Industry Uses

A. General Uses of Social Security Numbers

- *To assist in account administration and better respond to customer requests.* Financial institutions must use shared information to create central databases that then permit institutions to better respond to customer requests or needs (e.g., provide account balances, correct inaccuracies, process loan requests, etc.). To do this, many institutions use social security numbers as a unique identifier to ensure more accurate records.
- *To combat fraud and identity theft.* Financial institutions rely on third-party databases to investigate claims of fraud and identity theft. These third-party databases in turn rely on social security numbers as the common unique identifier that is used by a variety of data sources. Without such common unique identifiers, there would be no way to ensure that particular information is associated with a particular individual, and not with someone posing as that individual. Thus, SSNs are integral mechanisms for accumulating and processing authentic information for both law enforcement officials and financial institutions.
- *To accurately assess risk.* Everyday, financial institutions make judgments regarding financial risks. Institutions must rely on information databases to make such judgments, whether they are decisions on loans, insurance products, or other financial services. Social security numbers, when used by internal and third-party data providers as a means of compiling accurate information on an individual, help institutions make prudent decisions on product offerings.
- *To verify the identity of the customer—in person, over the phone, by mail, or over the internet—in the account opening stage.* A financial institution uses a social security number as the unique individual identifier when verifying information of a person with whom the institution has had no previous contact.
- *To identify potential terrorist funding and money laundering activities.* Institutions use social security numbers as unique identifiers to comply with various government requirements, such as the U.S.A. Patriot Act, Office of Foreign Assets Control (OFAC) verifications or the processing of certain Bank Secrecy Act-related documents (e.g., cash transaction reports).
- *To meet other government safety and soundness requirements.* Federal and State bank regulators require banks and savings associations to operate in a safe and sound manner, and require institutions to develop sophisticated internal policies and procedures to that end. To do so, banks often rely on third-party databases that themselves rely on social security numbers to promote accuracy. As a result, the use of social security numbers plays a significant role in bank internal risk activities.
- *When providing tax reporting information* to the Government (e.g., Forms 1098/1099), as well as to the employee (e.g., W-2s).
- *To facilitate internet banking operations.* Many third-party vendors who provide links to such services rely on social security numbers as account identifiers.
- *To assist in internal security operations.* Institutions use social security numbers as an employee identifier for purposes of background checks and other activities.
- *To assist in internal benefits tracking.* For example, to provide reimbursements to employees incurring business expenses, or to track employee participation in employee retirement funds (e.g., 401(k) plans).
- *To track external payments to vendors for tax reporting purposes.*
- *To permit customer access to a wide range of 24-hour banking services via phone or internet.* Many banks use social security numbers as the account identifier, both as a convenience to customers and to maintain consistency with other internal processing needs, such as the maintenance of an accurate central database and the subsequent ability to use such numbers when making external credit checks.

B. Type of Institutions that Benefit

- *To facilitate financial holding company operations of benefit to the company and its customers.* Holding companies share customer information (including social

security numbers) within their corporate family (i.e., affiliates) for a variety of purposes, including:

- *Providing customers with consolidated statements reflecting the status of all of their financial accounts and investments.* To do so, companies need to ensure that customer information matches the correct file—e.g., that the "John Smith" on the phone is the John Smith that has two checking accounts, a variable life insurance policy, and holds the securities of four particular companies. Using social security numbers—the only truly common unique identifier—to verify this information greatly enhances company accuracy and increases customer confidence.
- *Assisting each affiliate in combating identity theft* by giving these affiliates necessary information on the customer so that they may protect the customer's interest. For example, having accurate, up-to-the-minute customer information allows affiliates to quickly identify inconsistencies or irregular activities in a customer's accounts that may reflect that identity theft is occurring. Again, reliance on social security numbers as the "common" element that permits institutions to cross-check existing customer information with new information helps institutions help their customers.
- *Allowing all aspects of the company to prudently manage risk.* When a customer enters a bank, insurance company or securities firm in search of a financial product or service, a financial institution must quickly and accurately gauge its financial risks in providing that product or service. The institution must rely on a variety of credible internal and external databases, such as those provided by credit bureaus, third-party vendors and other affiliates, for accurate information on the credit standing and financial health of the applicant. To ensure that these databases are as accurate as possible, such providers must rely upon some form of common identifier that ensures that correct financial history information is associated with the right person. Social security numbers, as the most accurate common identifier available, help ensure the highest available level of accuracy in these databases. Since a financial institution can then rely on the accuracy of this information in assessing its risk, it can make quick, efficient and prudent decisions regarding the new customer.

B. Securities Industry Uses

- *Account identification.* Many securities firms' systems rely heavily on social security numbers for identification. In general, account relationships are maintained based on SSN as the sole unique identifier for an individual.
- *Tax reporting.* SSNs appear on account opening documentation, primarily for tax reporting purposes.
- *Telephone verification.* Firms use SSNs to verify the identity of a client transacting business over the telephone—this enables firms to access an account by keying in the SSN if the customer does not remember his/her account number.
- *Account searches.* Firms use SSNs for account searches, thus enabling firms to sort all accounts for a customer under the same SSN.
- *Court Actions/Judicial Process/Subpoenas.* Securities firms are often required to provide documents, which would reveal SSNs of a client in responding to a subpoena, court order, or judicial process. Firms also use SSNs to search for accounts in response to requests from regulators and law enforcement officials.
- *Securities law reporting.* Many of the reports securities firms are required to file with the SEC and self regulatory organizations are based on SSN searches and identify SSNs. For example, certain reports to stock exchanges are based on total positions by related party (i.e., SSN).
- *Institutional risk control/anti-fraud.* Firms may use SSNs to perform anti-fraud background checks on potential clients in order to determine whether for example the person has a history of defrauding others.
- *Compliance.* SSNs are used to identify certain types of activity that firms are required to conduct surveillance for, such as excessive turnover in accounts.
- *Communications to shareholders.* SSNs are used in connection with mutual fund mailings, including the mailing of proxy statements and prospectuses to proprietary fund shareholders. SSNs are also used in connection with dissemination of a company's annual report, quarterly report, or interim report.
- *Escheatment/Abandoned Property.* Securities firms are required to provide on an annual basis to individual States the name, last known address, SSN, and other information for purposes of complying with various State escheatment and abandoned property laws, and intangible property tax laws.
- *Transfers of accounts to third parties.* SSNs are used to facilitate a customer request to transfer an account to another securities firm, or to satisfy a customer

request that a physical stock certificate be transferred from street name into his or her name.

- *Insurance.* SSNs may also be disclosed where a client purchases an insurance policy through the securities firm—the securities firms would then have to disclose (through the client's application) information, including SSN, to the insurance company.

C. Insurance Industry Uses:

1. Property/Casualty Insurers' Use of Social Security Numbers

- To the extent the p/c insurance industry uses SSNs, that use is confined to legitimate business practices such as underwriting policies, complying with numerous state and federal laws, and verification of identity.
- A proposal to prohibit or limit the disclosure of SSN could restrict p/c insurers from obtaining necessary information for underwriting and verification purposes.
  - For example, auto insurers use motor vehicle records to assess insurance risks, reevaluate risks undertaken, conduct claims fraud investigations and pay injured victims. Motor vehicle records, which include social security numbers as identifiers, are an essential source of information needed by insurers to comply with state consumer protection laws and existing contracts.
  - Auto insurers may use SSNs obtained from the consumer in order to verify the receipt of proper Department of Motor Vehicle records.
- Undue restrictions on use of SSNs could also impair the ability of p/c insurers to comply with reporting requirements under current federal and state laws, such as those described below.
  - Federal laws require p/c insurers to report certain payments with the claimant's SSN to the IRS.
  - P/C insurers are required under the Federal Welfare Reform Act to report to state welfare agencies certain information, including SSNs, so that the state can seize settlement dollars from non-custodial parents.
  - Under state workers compensation laws, p/c insurers are required to file accident claims (which include the claimant's SSN) with various agencies for those agencies' claims administration purposes.
  - States laws require p/c insurers to disclose to state-licensed advisory organizations certain information, which may include a SSN. The state-licensed advisory organizations perform a critical function in insurance pricing by using the information to conduct actuarial projections of anticipated losses so that state insurance regulators are able to perform their duties and insurance companies can establish rates in accordance with state-approved rating systems.

2. Life, Disability Income, and Long Term Care Insurers' Use of Social Security Numbers

Life, disability income, and long term care insurers are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. However, in order for insurers to serve their prospective and existing customers, they must use and share nonpublic personal information, including social security numbers, in connection with the origination, administration, and servicing of insurance products and services. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. Life, disability income, and long term care insurers also believe that the use and responsible sharing of nonpublic personal information, including social security numbers, generally increases efficiency, reduces costs, and makes it possible to offer economies and innovative products and services to consumers that otherwise would not be available.

a) Underwriting life, disability income, and long-term care insurance policies—Insurers must be able to obtain and use nonpublic personal information, including SSNs, in order to underwrite applications for coverage. SSNs are used in a number of different ways in connection with this process:

- *To obtain verifiable medical information.* Insurers sometimes must use proposed insureds' SSNs in order to obtain medical information about them from doctors and hospitals which use SSNs as identification numbers.
- *To obtain drivers' record information.* Insurers sometimes use motor vehicle record information in underwriting. In some states, insurers are required to use SSNs to obtain this information from the motor vehicle department.

- *To obtain credit report information.* Insurers sometimes use information from credit reporting agencies in underwriting, and SSNs are sometimes required to obtain information from consumer reporting agencies.

b) Performance of Essential Insurance Business Functions—Once life, disability income, or long term care insurance policies are issued, insurers use their customers' nonpublic personal information, including their social security numbers, to perform essential, core functions associated with insurance contracts, such as for claims evaluations and policy administration. The ability to use this information for these purposes is crucial to insurers' ability to meet their contractual obligations to their customers and to perform important related service and administrative functions. They use SSNs to perform a number of these core insurance business functions, which include the following:

- *To locate policyholders.* SSNs are used by insurers to find missing or lost policyholders to inform them that they are entitled to life insurance proceeds.
- *For customer service.* SSNs are used to identify policies owned by an individual who does not have the account or policy number available when a service request is made.
- *For phone call verification.* Insurer call centers use SSNs as part of the data requested to authenticate customers who call with requests for service or for product or account information or status.
- *To transfer assets to unaffiliated financial institutions.* SSNs are often needed to transfer assets from one financial institution to another, for example, for purposes of transfers between mutual funds or annuities and life insurance. (Since one financial institution generally does not know an individual's account number at another financial institution, the SSN is needed to identify the client's identity for the two institutions. This reduces delay, error, and misplaced assets in such transfers.)
- *Pension plan administration.* Insurers also use SSNs in connection with the administration of pension plans, as identification numbers.
- *For online services.* Insurers use SSNs as PIN numbers for customers' use of online services.
- *As identification for group insurance plans.* Insurers use SSNs in reporting to employer policyholders under employee group insurance plans and in connection with payroll deductions under these plans.

c) Disclosures Pursuant to Regulatory/Legal Mandates or to Achieve Certain Public Policy Goals—In furtherance of public policy goals designed to protect American insurance consumers, life, disability income, and long term care insurers share nonpublic personal information, including SSNs, to:

- *State insurance departments* to assist them in their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers;
- *Self-regulatory organizations,* such as the Insurance Marketplace Standards Association (IMSA), which impose and monitor adherence to requirements with respect to member insurers' conduct in the marketplace; and
- *State insurance guaranty funds,* which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information.

Any limitation on these disclosures would seem likely to operate counter to the underlying public policy reasons for which they were originally mandated—to protect consumers.

Life, disability income, and long term care insurers are also required to make certain disclosures of information by the federal government. In addition, they need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies and state insurance departments. Their primary purpose is to reduce the cost of insurance by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. Any limitation on insurers' right to make these disclosures would seem likely to undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.

Life, disability income, and long term care are required to use SSNs to report to the IRS a variety of payments to insurance consumers, including, but not limited to, interest payments, certain dividends, and policy withdrawals and surrenders. At least one state, Rhode Island, requires that insurers match "deadbeat" parents data before making payments on claims. SSNs are required for that matching.

d) Ordinary Business Transactions—In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Nat-

urally, these files can contain personal information, including customers' SSNs. Such disclosures are often necessary to the due diligence process that takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly-created entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements often necessitate the disclosure of personal information, which may include SSNs, by the primary insurer to the reinsurer.

PREPARED STATEMENT OF PATRICK P. O'CARROLL, ACTING INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Good morning, Chairman Stearns, Ranking Member Schakowsky, and members of the Subcommittee. Thank you for the opportunity to provide a statement for this important hearing to discuss the complex problem of protecting private consumers' Social Security number (SSN) from misuse and the Committee's proposed legislation, the *Social Security Number Privacy and Identity Theft Prevention Act of 2004.*

The SSN as a National Identifier

I would like to begin my statement today with a simple declaration: The SSN is a national identifier. In past years, many would challenge that comment. Today, we live in a changed world, and the SSN's role as a national identifier is a recognized fact. Unfortunately, with that knowledge, we must also accept that because the SSN is so heavily relied upon as an identifier, it is a valuable commodity for lawbreakers. Given the importance of this unique, nine-digit number and the tremendous risk associated with its misuse, one of the most important responsibilities my office undertakes each day is oversight of SSN integrity.

Today I would like to focus my testimony on how the SSN is misused to commit crimes, my office's role in addressing homeland security and identity theft, and what more needs to be done to ensure the integrity of the SSN. The protection of private consumers' SSNs is an important concern in fighting identity theft and safeguarding SSN integrity. Over the years, we have raised concerns in testimony and reports and have called for improved security for *all* databases—both public and private sector—that contain SSNs and other sensitive data, both as a homeland security issue and as an identity theft issue.

The SSN is a widely used identifier, which can be used to tie multiple records together about a single individual. While phone numbers, addresses, and even names can change, the SSN is constant throughout an individual's life. Because of this, many institutions, including hospitals and some banks and brokerages, use clients' SSNs as an identity confirmation. Other institutions, notably banks, use SSNs as secret passwords that only the owner should know.

While common use of the SSN as an identifier seems reasonable, it is an invitation for identity theft. For example, if someone knows the name and SSN of another individual, they could use this information to access accounts, transfer funds, or make other changes to an account, which may have serious repercussions for the true account holder. When SSNs appear with their owners' names on driver's licenses, mailing labels, and university student ID cards, the owners of these SSNs become potential targets. In fact, we are currently reviewing the use of the SSN on student IDs in a nationwide audit that will examine such policies at approximately 100 schools. Perhaps the most important step we can take in preventing SSN misuse is to limit the SSNs easy availability on public documents, and even in electronic forums such as the Internet.

Our investigations in this area reveal how widespread the misuse of SSNs and other sensitive data from public and private sector databases has become. For example, we recently discovered an offer to sell up to 10,000 SSNs with matching names on the eBay web site. These SSNs were used by the University of North Carolina at Pembroke as identifiers for its staff, current students, and applicants. The suspect successfully stole these SSNs and was ultimately sentenced to 5 months' incarceration.

Our Philadelphia Field Division participated in an investigation that found that a former credit card company employee provided several co-conspirators personal information of legitimate account holders. The co-conspirators then used this information to open and transfer money from fraudulent accounts. The former employee was sentenced to 4 years probation and ordered to pay the bank restitution of over $132,800.

In another case, after a year-long identity theft investigation, our agents arrested a man who had more than 250 credit cards—along with identification documents and fraudulent Social Security cards—for aliases he used in an elaborate scheme he began while working as a credit manager at a local furniture store. When the company was sold and his job was terminated, he took several credit reports with him and used those SSNs to get credit cards, bank loans, homes, vehicles, computers and cash. He was sentenced to 25 months in prison, ordered to pay $383,000 in restitution to numerous credit card companies and banking institutions, and ordered to forfeit a home and a recreational vehicle.

The range of sources from which these SSNs and other critical personal information were stolen is alarming—legitimate web sites, universities, credit card companies, and a furniture store. It is not just SSA that has your number—numerous government agencies, companies and individual operators such as doctors and insurance agents have them as well. In fact, it is quite possible that your number has been given without your knowledge to numerous organizations, businesses and individuals. We cannot put the genie back in the bottle, but we must do more to make those who hold this critical information treat it with the same respect they would give to their own bank account numbers.

Misuse of the SSN to Commit Crimes

For those with an illicit motive, an SSN can be obtained in many ways:

- Presenting false documentation to the Social Security Administration (SSA).
- Stealing another person's SSN.
- Purchasing an SSN on the black market.
- Using the SSN of a deceased individual.
- Creating a nine-digit number out of thin air.

Although SSA may never be able to completely prevent individuals from purchasing an SSN on the black market or stealing the SSN of another, we are proud that our efforts are making it more difficult to do so.

For example, based on an investigation conducted by our Atlanta Field Division, a St. Petersburg, Florida resident was recently sentenced to 27 months of incarceration and ordered to make restitution to SSA for over $79,000 in survivors benefits she received for herself and three nonexistent children. To perpetrate this scheme, the individual assumed the identity of a former acquaintance by obtaining a North Carolina identification card in her friend's name. With this new identity, she used fraudulent birth certificates to apply for SSNs on behalf of two fictitious children. She also altered court marriage and divorce documents, falsely claiming that a known deceased man was her ex-husband and the fictitious children's father. She perpetrated this elaborate scheme so that she could apply for and receive Social Security survivors benefits for the fictitious children—and, until caught, was successful in doing so. Further investigation revealed that she had previously committed a similar crime resulting in additional survivors benefits for herself and another fictitious child.

Other Federal agencies such as the Department of Housing and Urban Development (HUD) have also experienced a significant increase in the number of identity theft occurrences in their programs. Within programs administered by HUD, identity thieves are using someone else's SSN to obtain and then default on home mortgages—leaving taxpayers to pay their bills.

Our Role in Addressing Homeland Security and Identity Theft

Recognizing the importance of SSNs to terrorists and identity thieves, SSA and my office, the Office of the Inspector General (OIG) take very seriously our responsibility to ensure that these numbers are only issued to those with a legal reason for having one. As such, we continuously seek innovative ways to prevent SSN misuse and create collaborative partnerships with other Federal, State, and local entities to address both homeland security and identity theft concerns.

OIG Homeland Security Activities

While financial crimes involving SSN misuse are more numerous than terrorism-related crimes, the potential threat to homeland security nevertheless justifies intense concern. Because SSNs allow individuals to assimilate themselves into U.S. society, these numbers can become valuable tools for terrorists or others who wish to live in the United States and operate under the "radar screen." Once an individual has an SSN, he has the ability to work, buy a home, and engage in a wide range of financial transactions including the raising and transferring of funds.

Our active involvement in addressing homeland security began on September 11, 2001, with our agents assisting in rescue efforts and site security at the World Trade Center. We immediately assigned supervisors and agents to the FBI Com-

mand Centers in New York City and New Jersey to process information and investigate leads. The Inspector General ordered all Field Divisions to assist in Joint Terrorism Task Forces (JTTF) and Anti-Terrorism Task Forces (ATTF) around the country—in fact, we are now active participants in 63—Joint Terrorism Task Forces and 29 Anti-Terrorism Task Forces, as well as the Foreign Terrorist Tracking Task Force.

In carrying out our homeland security responsibility, we coordinate closely with other Federal agencies. For example, we recently met with representatives of the Department of Homeland Security (DHS) to discuss methods in which we could work together to address the SSN's role in homeland security. We welcome this opportunity and believe cooperative ventures such as these are imperative to ensure that all of the links in the homeland security chain stay connected. Based on our initial discussions, we plan to work with DHS to explore possible data matching and cross-verification opportunities—those that are currently provided for under law and those for which additional legislation may be required.

We are also coordinating with DHS and the Department of State (State) to review the effectiveness of the Enumeration at Entry initiative, a collaborative effort among the three agencies to facilitate the issuance of SSNs to legally admitted aliens whose immigration status permits such issuance. This initiative is designed to ensure that DHS and State certify the identity and immigration status of an alien before an SSN is assigned to that individual. Further, we have worked with the Department of Defense to determine whether individuals having public responsibilities and positions, primarily active duty military personnel, have reported wages with names and/or SSNs that do not match SSA's records. We are concerned about both unknown individuals working for the military branches and potential SSN misuse by military employees.

OIG Identity Theft Activities

I am also concerned about the escalating occurrences of identity theft, which is the fastest-growing form of white-collar crime in the United States. In September 2003, the Federal Trade Commission (FTC) released a survey showing that 27.3 million Americans were victims of identity theft between 1998 and 2003—including 9.9 million people in the study's final year. FTC also reported that during the study's final year, losses to businesses and financial institutions totaled nearly $48—billion and consumer victims reported $5—billion in out-of-pocket expenses. Clearly, this is an epidemic that must be brought under control.

Identity theft is an "enabling" crime, one that facilitates other types of crime, ranging from passing bad checks and defrauding credit card companies to committing acts of terrorism. Additionally, criminals use identity theft to defraud Federal agencies and programs of millions of dollars.

By law and by mission, our office has a narrow but important role in the overall effort to address identity theft. Much of the Federal government's responsibility for identity theft issues has been assigned by Congress to the FTC. State and local law enforcement agencies and financial institutions also have critical roles to play.

Because our primary mission is to protect the integrity of SSA's programs and operations, in the majority of our identity theft investigations, we continue to focus investigative efforts on cases that affect SSN integrity. For example, our Chicago Field Division took part in a 3-day inter-agency undercover operation that resulted in the arrest of 12 suspects dealing in fraudulently obtained Social Security cards, State driver's licenses, and U.S. passports. Our investigators determined that the group's leader and 11 others took part in an elaborate document-counterfeiting scheme to obtain valid SSNs for non-existent children. The names belonged to undocumented noncitizens who paid up to $5,000 each for valid documents. Members of the group were sentenced to up to 2 years in prison or given immunity from prosecution for their cooperation in the undercover sting.

To maximize our investigative resources, we dedicate agents that work on task forces with other law enforcement agencies nationwide to investigate identity crimes. We also work closely with prosecutors to bundle SSN misuse cases that, when presented separately, may not have been accepted for prosecution.

We are also continuing our efforts to identify opportunities for SSA to further strengthen the integrity of the SSN. One of my major concerns has been the use of fraudulent documents to obtain SSNs. We continue to explore and recommend further controls the Agency can implement to strengthen SSA's important responsibility of assigning SSNs.

SSA Initiatives to Address SSN Integrity

SSA has made significant progress in strengthening the defenses of the SSN, implementing important suggestions our office has made, and working with us to find

solutions. In November 2001, the Commissioner of Social Security established an Enumeration Response Team (ERT) comprised of executives from throughout the Agency, including representatives from the OIG. The Commissioner charged this group with identifying steps the Agency could take to improve the enumeration process and to enhance the integrity of the SSN. Since that time, the Commissioner and the ERT have implemented numerous policies and procedures designed to better ensure that only individuals authorized to do so, receive an SSN. For example, the ERT recommended, and SSA adopted, more stringent circumstances under which an individual may obtain a non-work SSN. We are proud to serve on workgroups such as these and applaud the Commissioner and SSA for their strong commitment to improving SSN integrity.

Prior to the ERT, the Agency implemented other initiatives such as the Comprehensive Integrity Review Process (CIRP) and Enumeration at Entry process. The CIRP system identifies vulnerabilities in the enumeration process and issues alerts to SSA's field offices (FO) to develop and certify. The FO reviewer, usually a manager or supervisor, performs an enumeration integrity review of each alert. If the reviewer determines that there is a possibility of fraud, the alert is forwarded to the OIG for development and disposition.

What Actions Still Need to Be Taken to Address SSN Misuse

Despite the significant progress SSA and Congress have made in recent years to address SSN misuse, we believe SSN integrity and protection still need improvement at three stages: at issuance, during the life of the number-holder, and following the number-holder's death.

At Stage One (issuance of the SSN), my office is working closely with Congress and SSA to strengthen controls over the enumeration process, ensure the integrity of identification documents, and make it as difficult as possible to fraudulently obtain an SSN from the Federal government. Together with Congress and with SSA, we have made important strides in reducing enumeration vulnerabilities, and that effort continues. Still, to strengthen our defenses even further, we believe SSA should implement the following changes.

- Continue to address identified weaknesses within the enumeration process to better safeguard SSNs.
- Work with State Bureaus of Vital Statistics to incorporate additional controls in SSA's Enumeration-at-Birth program, such as periodically reconciling the number of SSNs assigned through the program to the number of births reported by participating hospitals.

In the last several years, we have focused significant resources to address SSN protection within Stages Two (during the life of the number holder) and Three (after the number holder's death). Specifically, we have conducted numerous audits and made extensive recommendations to SSA to improve the SSN misuse problem in the earnings reporting process, and most importantly, to improve controls over SSN misuse as it pertains specifically to Homeland Security. Nevertheless, to more completely address SSN integrity during the life of the number holder and following that number holder's death, we believe SSA and lawmakers should examine the feasibility of the following initiatives.

- Limiting the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.
- Prohibiting the sale of SSNs, prohibiting their display on public records, and limiting their use to legitimate transactions.
- Enacting strong enforcement mechanisms and stiffer penalties to further discourage SSN misuse.
- Cross-verifying all legitimate databases that use the SSN as a key data element.
- Review the implications of releasing information on deceased individuals.

Limiting the SSN's Public Availability and Sale of the SSN

Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability. We believe legislation designed to protect the SSN must strictly limit the number's availability on public documents. As long as criminals can walk into the records room of a courthouse or local government building and walk out with names and SSNs culled from public records, it will be extremely difficult to reverse the growing trend of SSN misuse. We also believe effective legislation should also specifically prohibit the sale of SSNs—including one's own SSN—on the open market. In addition, as long as criminals can buy a list of names and SSNs through an Internet auction, we will continue to be plagued by the consequences.

To be fully effective, we also believe legislation must limit the use of the SSN to appropriate and valid transactions. The financial industry relies on the SSN, and

no one is suggesting that we change the way legitimate business is conducted in the United States. But the use of the SSN as a student or patient identification number, as part of a car rental contract or to rent a video, must be curtailed.

Congress enacted the *Identity Theft and Assumption Deterrence Act of 1998,* P.L. 105-318, responding to the growing epidemic of identity thefts by imposing criminal sanctions for those who create a false identity or misappropriate someone else's. The *Internet False Identification Prevention Act of 2000,* P.L. 106-578, closed a loophole left by the earlier legislation, enabling our office and other law enforcement organizations to pursue vendors who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents. More legislative tools are needed, and we have worked with Congress to identify legislation necessary to protect the integrity of the SSN. For example, the House is now considering H.R.—2971, the *Social Security Number Privacy and Identity Theft Prevention Act of 2004,* which would restrict the use of SSNs in the private and public sector, and criminalize the sale of SSNs.

Penalties

The identity theft legislation I discussed earlier provides criminal penalties, but those penalties were designed for identity theft crimes involving Social Security cards and/or SSNs, not for SSN misuse itself. We believe legislation should not only provide criminal penalties for those who misuse SSNs, but should also provide criminal penalties for those few SSA employees who betray the public trust and assist criminals in improperly obtaining SSNs.

For example, a former SSA Service Representative was sentenced to 3 years probation and community service after pleading guilty to a bribery charge in connection with issuing 100 to 200 Social Security cards to illegal aliens. She received between $50 and $150 for each card. We believe it is critically important to send a strong message to SSA employees tempted to facilitate crimes against Agency programs by pursuing the maximum sentence possible.

On July 15, 2004, the President signed the *Identity Theft Penalty Enhancement Act,* P.L. 108-275, into law, establishing enhanced penalties for aggravated identity theft. While increased criminal penalties are a welcomed addition to the arsenal available for use in combating identity theft, we also believe legislation should provide an administrative safety net in the form of Civil Monetary Penalties to allow for some form of relief when criminal prosecution is not available for SSN misuse and other Social Security-related crimes.

Cross-verification

Additionally, we strongly support cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies. Our experience has shown that cross-verification can combat and limit the spread of false identification and SSN misuse. Further, we believe all law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. In doing so, the law enforcement community would use data already available to the Federal, State and local governments and the financial sector.

Potentially, the rewards of cross-verification can be great, and it would not require major expenditures of money or the creation of new offices or agencies. We believe legislation is needed toexpand cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. To offset SSA's cost for providing such services, the Agency could charge a modest fee to commercial and financial entities. The technology to accomplish these data matches and verifications exists now. Coupled with steps already underway by SSA to strengthen the integrity of its enumeration business process, cross-verification, once initiated, would be a critical step in combating the spread of identity fraud.

Let me give you an example of an identity theft case in which cross-verification may have prevented a crime against a Federal government program, saving taxpayers $62,000. A Salt Lake City grandmother learned last year from one of my Denver Field Division agents that her SSN was used to purchase a $146,000 HUD home. This identity theft went undiscovered until the home went into foreclosure because the criminals used this grandmother's SSN, but another name to purchase the home. Had HUD been allowed to verify the accuracy of the borrower's name and SSN with SSA, HUD would have recognized the discrepancy and denied the loan. In this one case alone, the Government would have saved the thousands of program dollars HUD had to pay to foreclose and resell the property. Additionally, this elderly Salt Lake City grandmother would have been spared the time and expense of repairing her credit record.

We believe cross-verification is one of the most important tools the Government and private sector can employ to reduce the instances of identity theft. We understand the important issue of consumer privacy that must be considered by Congress and others before allowing such data integrity matches. However, our ability to prevent these egregious crimes would be enhanced by additional legislation balancing the need for consumer privacy with the need for accurate identifying information.

Conclusion

We appreciate the invitation to provide a statement to this Subcommittee and to assist you in the very important work you are doing to help protect consumers' SSNs. We are very pleased with the progress Congress and SSA have made in addressing the issue of SSN integrity over the last several years. However, we reiterate our concern that more must be done to ensure that only those individuals authorized to have an SSN receive one and that anyone who fraudulently obtains and misuses an SSN is adequately penalized. As such, we believe recently enacted legislation such as P.L. 108-275, the *Identity Theft Penalty Enhancement Act*, is a significant step toward holding accountable individuals who misuse SSNs to commit egregious crimes. In addition, we support legislation such as H.R. 2971, the *Social Security Number Privacy and Identity Theft Prevention Act of 2004*, which severely limits the sale, purchase and display of SSNs to the general public.

We also ask that Congress consider other measures such as increased cross-verification among Government and private sector entities, Civil Monetary Penalties for SSN misuse and other Social Security-related crimes when criminal prosecution is not available, and stronger penalties for those few SSA employees that betray the public trust by selling SSNs. We will certainly continue our vigilance in addressing these issues and stand ready to do more to enhance the safety and well-being of all Americans.

FEDERAL TRADE COMMISSION
October 20, 2004

The Honorable CLIFF STEARNS, *Chairman*
Subcommittee on Commerce, Trade and Consumer Protection
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

DEAR MR. CHAIRMAN: Thank you for the opportunity to present the views of the Federal Trade Commission at the September 28, 2004, hearing of the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce, on H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2004. This letter responds to the Subcommittee's request for more specific views on the bill itself. In addition, the letter addresses Representative Green's question at the hearing about the length of time that a fraud alert remains on a consumer's credit file.

As I stated at the hearing, I believe that the goals of H.R. 2971 are laudable. It seeks to strike the right balance between the legitimate and permissible sale and display of Social Security numbers (SSNs) and those that should be eliminated. It is extremely difficult, however, to find the correct place to draw the lines, by rulemaking or otherwise. Some provisions, like restrictions on access by prisoners, are clearly justified, but others may have unintended consequences. I believe that this bill, if enacted in its current form, would present significant challenges to the credit granting system and may ultimately harm consumers. The primary concern in this regard is with Sections 109 and 110. Below, I provide a brief analysis of these provisions and their potential negative impact on consumers.

In my oral presentation, I mentioned that there are many legitimate uses of SSNs in commerce that provide substantial benefits to consumers. In particular, SSNs are used by consumer reporting agencies (*e.g.*, credit bureaus) to organize consumer data files and to match individual consumers with the correct consumer file (*e.g.*, credit report). In order to ensure accurate and complete results, it is important for consumer reporting agencies to obtain a consumer's SSN from those that request the consumer's credit report.[1] Similarly, when financial institutions report account information to consumer reporting agencies, the SSN is used to match that informa-

[1] The FTC is required, under the Fair and Accurate Credit Transactions Act (the FACT Act), to study the processes by which consumer reporting agencies "match" consumer files to particular consumers prior to releasing a consumer report to a user. *See* Pub. L. No. 108-159 § 318. That study will be completed in December 2004. It is clear, however, that the current consumer reporting system relies heavily on consumers' full SSNs.

tion to the correct consumer file. Without SSNs, consumer reporting agencies may be unable to accurately match individual consumers with the proper credit reports, and may be unable to match information from financial institution records to individual consumer files. This could cause inaccurate information to appear in individual consumer files and errors in reporting the wrong file to inquiring creditors and other permissible users. Thus, undue restrictions on the availability of SSNs to businesses could harm consumers by diminishing the accuracy of the consumer reporting system.

In addition, many businesses rely on SSNs to obtain current address and other contact information on consumers for a number of legitimate purposes. For example, a business may need a consumer's current address information in order to administer rebate, recall, or consumer redress programs; locate beneficiaries, lost heirs, or the holders of dormant accounts; and perform collection activities. In addition, this information is often used for law enforcement and public safety investigations. Consumer reporting agencies generally possess the most up-to-date consumer address and contact information. Because SSNs play an important role in the consumer reporting agencies' ability to match an individual consumer with the information relating to him, it would be more difficult for businesses and law enforcement without SSNs to obtain consumers' current address and contact information for a variety of legitimate purposes.

This does not mean that consumer reporting agencies should be able to use SSNs without restriction. In my view, however, H.R. 2971 in its current form could eliminate or hinder legitimate uses of SSNs, to the ultimate detriment of consumers.

Section 109

Section 109 of H.R. 2971 would restrict consumer reporting agencies from disclosing SSNs except as part of a "full consumer report" (*i.e.*, where there is a permissible purpose under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, (FCRA)). Under the FCRA, businesses may obtain from consumer reporting agencies identifying information about consumers (often referred to as "above the line" information), including SSNs, without having one of the permissible purposes specified in the statute.[2] By prohibiting consumer reporting agencies from furnishing SSNs except as part of a full consumer report, Section 109 would cut off use of SSNs for many legitimate uses, such as law enforcement, public safety investigations, and insurance or pension benefit distributions,[3] which are not permissible purposes for full file disclosures under the FCRA.[4]

At the same time, in those situations where a business does have an FCRA permissible purpose for a full file disclosure, this section could encourage the overdisclosure of consumer information, because a business with a need for SSNs in order to obtain, for example, current address information, would be forced to purchase a full consumer report containing much more sensitive information than the user needs. In sum, this provision could have a negative impact on the availability of accurate consumer identifying information for legitimate uses, in addition to overdisclosing sensitive consumer information in other instances.

Section 110

Section 110 of H.R. 2971 would make it unlawful for a business to require an individual to provide his SSN as a condition of doing business, and to do so would vio-

---

[2] This identifying information generally is not covered by the FCRA. *See FTC v. Trans Union*, Dkt. 9255, Op. of the Commission at pp. 30-31 (Mar. 1, 2000) (holding that consumer name, SSN, address, telephone number, and mother's maiden name do not constitute a consumer report under the FCRA).

[3] For example, assume that a consumer purchases life insurance. In current practice, the insurer generally would require the purchaser to provide his SSN, as well as those of any beneficiaries. When the policy matures and the insurer seeks to locate the beneficiaries, the insurer typically would use the SSNs it had collected previously to find the current address information for those beneficiaries through a consumer reporting agency or other commercial database. Section 110 would prevent the insurer from requiring the SSNs of the consumer and the beneficiaries at the time the policy is purchased. Without the SSNs, the insurer could not obtain current address information for the beneficiaries from a consumer reporting agency, because the insurer likely would not have a permissible purpose to obtain their full consumer reports.

[4] Apart from the FCRA, the disclosure of SSNs by consumer reporting agencies and other financial institutions is limited under the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions (with certain exceptions) to provide consumers with notice and an opt-out opportunity before sharing personal financial information with nonaffiliated third parties. *See* 16 C.F.R. Part 313. However, the exceptions to the GLBA notice and opt out requirements allow many legitimate business uses and disclosures of this information, including for law enforcement and public safety investigations. *See* 16 C.F.R. §§313.14-.15. The permissible purposes under the FCRA that would govern disclosure of SSNs under H.R. 2971 are significantly narrower than the GLBA exceptions.

late Section 5 of the FTC Act. The only exception to this provision is for circumstances where the business is expressly required under federal law to submit the individual's SSN to the federal government. As you know, this exception is very limited and would not allow businesses to require SSNs for many legitimate uses. For example, Section 110 would prevent creditors, insurers, and others from requiring a consumer to provide an SSN in connection with an application for credit, insurance, or other business transaction involving the consumer. As a result, this section would hinder the ability of businesses to obtain credit reports for legitimate purposes, such as risk analysis, underwriting functions, and security checks.

In addition, similar to Section 109, this provision would prevent businesses with a legitimate need for consumers' current address information from obtaining that information, because that information is generally only accessible with an SSN.

Thus, for the reasons described above, I believe that Section 110 could have a significant negative impact on consumers.[5]

Fraud Alerts Under the FACT Act

Finally, during the hearing, Representative Gene Green asked about the length of time that a fraud alert—that is, a notation that the consumer is a potential victim of identity theft or fraud—remains on a consumer's credit file. At present, as a voluntary practice, the nationwide consumer reporting agencies have been using a two-step fraud alert system, placing initial and extended fraud alerts in consumers' files upon request. The first national consumer reporting agency contacted notifies the other two of a consumer's request for an initial fraud alert. If the consumer later seeks to have an extended alert placed in his file, he will have to contact each of the three agencies. The duration of the initial fraud alert has varied among the agencies from 90 days to twelve months. All three agencies have left the extended fraud alert in the consumer's file for seven years.

The FACT Act codifies and expands upon these voluntary practices. The fraud alert provisions go into effect on December 1, 2004, and provide for a two-step fraud alert system.[6] Upon the initial request of a consumer, a nationwide consumer reporting agency must include an initial fraud alert in that consumer's file for not less than 90 days. If that consumer subsequently requests an extended alert and submits an identity theft report,[7] a nationwide consumer reporting agency must include an extended fraud alert in the consumer's file for seven years. A consumer may, however, request to have either type of fraud alert removed from his file prior to the expiration of the designated period. In addition, the nationwide consumer reporting agency receiving the request for the fraud alert, whether initial or extended, must refer the fraud alert information to the other nationwide consumer reporting agencies.

Thank you again for this opportunity to provide my views on H.R. 2971. I look forward to continuing to work with you on these important issues.

Sincerely,

THOMAS B. LEARY
Federal Trade Commission

---

[5] In addition, it would be valuable in the development of any legialation on this subject to have the results of the "matching study" that the FTC is conducting pursuant to the FACT Act. This study is intended to learn more about the processes by which consumer reporting agencies match consumer files to particular consumers prior to releasing a consumer report to a user. *See supra* n.1.

[6] Pub. L. No. 108-159 § 112; FCRA § 605A; 15 U.S.C. § 1681c-1.

[7] Under the FACT Act, the term "identity theft report" is to be defined by Commission rulemaking (*see* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act: Notice of Proposed Rulemaking and Request for Comment, 69 Fed. Reg. 23370, 23372 (Apr. 28, 2004)), and means, "at a minimum, a report that alleges an identity theft, is a copy of an official, valid report filed by the consumer with an appropriate Federal, state, or local law enforcement agency... the filing of which subjects the person filing the report to criminal penalties..." Pub. L. No. 108-159 § 112; FCRA § 603(q)(4); 15 U.S.C. § 1681a(q)(4).

○