S. HRG. 109–1089

IDENTITY THEFT

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 16, 2005

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

61–846 PDF WASHINGTON : 2010

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN McCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

WITNESSES

APPENDIX

IDENTITY THEFT

THURSDAY, JUNE 16, 2005

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. Gordon H. Smith, presiding.

OPENING STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH. Ladies and gentlemen, we welcome you to this hearing of the Senate Commerce Committee.

I thank our witnesses for being here today. Today's hearing takes place against the backdrop of one of the most rapidly growing crimes in America, identify theft. We'll hear from the Federal Trade Commission today that over ten million Americans are victimized by identity thieves every year. These numbers translate into losses of over $55 billion per year, averaging over $10,000 stolen per fraudulent incident.

In 2005 alone there were at least 43 known incidents of data breaches potentially affecting over 9 million individuals. In my own State of Oregon, we rank ninth in the Nation for fraud complaints and identity theft. These breaches range from sloppy recordkeeping and security procedures by companies to extremely sophisticated online thefts by computer hackers.

Last month, this Committee held a hearing on the recent data breaches at ChoicePoint, Inc., and LexisNexis, and methods used by private industry to prevent future data breaches. At today's hearing, the Committee will hear testimony concerning the current treatment of data broker services under existing state and Federal privacy laws, as well as proposals of public solutions to mitigate future data breaches and identity theft.

Protecting sensitive information is an issue of great importance for all Americans. Consumers should have confidence when they share their information with others that their information will be protected. At the same time, the ability of legitimate companies to access personal information certainly does facilitate commerce and continues to benefit consumers.

Data broker companies perform important commercial and public functions through their ability to quickly and securely access consumer data. Following today's hearing, I will be introducing legislation with my colleagues of this Committee. The principles of our bipartisan effort will include, one, a national obligation for companies to have a security procedure in place to safeguard sensitive and personal information, and, two, a balanced breach notification trigger to inform consumers when real risks of identity theft are at stake. We need to make sure that this legislation strikes the right balance to ensure the continued existence of the critical services while ensuring security of personal information to prevent its misuse and subsequent breaches and thefts.

I'd also like to pay a particular welcome to one of my fellow Oregonians, Congresswoman Darlene Hooley, who is here to share her thoughts with us today. She has been a great leader on this issue in the House of Representatives, and I appreciate, especially, her coming across the Hill to be with us today.

Before we turn to our first panel, it's my pleasure to turn the mike over to the Ranking Member of this Committee, Senator Daniel Inouye.

STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. Thank you very much, Mr. Chairman. I commend you for conducting this hearing.

I have a statement, but you've covered it adequately. I'd ask unanimous consent that it be placed in the record.

Senator SMITH. Without objection.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Data breach and identity theft is a serious problem that this Committee is committed to addressing. A 2003 Federal Trade Commission survey report found that during a 1-year period nearly 10 million Americans—or roughly 4.6 percent of the domestic adult population—were victimized by identity thieves. Public opinion polls consistently find strong support among Americans for privacy rights to protect their personal information.

The FTC and others have been working diligently to come up with a Federal legislative solution to protect America's consumers from the data breaches that lead to identity theft.

Any solution must include a provision that notifies consumers of data breaches so that they can protect themselves from the misuse of their personal information. In addition, consumers deserve to have certain rights in their dealings with the information industry, and to have those rights protected by their government.

Senator Bill Nelson has undertaken a tremendous amount of work on this issue, and I appreciate his interest and guidance. We are looking forward to working in bipartisan friendship with Chairman Stevens and Senator Smith to produce a bill that serves American consumers and allows them to take advantage of our great marketplace without fear.

Senator SMITH. Senator Burns, do you have an opening statement?

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. I do, and I shall be brief, Mr. Chairman.

I want to thank you and Senator Stevens for setting this hearing up today, and I want to congratulate you for all the hard work you've done on this issue. I don't think there's anybody in the country that I don't talk to that doesn't fear identity theft. We've had all kinds of news articles and information on identity theft and how it has harmed them with regard to credit cards and multiple other situations. It's timely.

And it is something that we've been dealing with here on this Committee a long time, all the way back to wherever we started to become really aware how big Internet commerce is and the dangers that were out there through the encryption debate, security and safety debates, and through spam and ham and everything else—we went through all of that—and yet we still have—problems keep cropping up about the shortfalls that we have been guilty of here in protecting people's security and, of course, their privacy. And privacy is utmost in the minds of a lot of people. They have a right to be concerned, and they're very angry about this situation.

I look forward to hearing the witnesses today. I also would—after these witnesses we can draw some sort of a conclusion that there might be legislation; and, if there is, I will be very supportive of what Senator Smith and the rest of the people in this Committee do, and would hope that we have some sort of input.

But we've also got to be careful on this issue, because we sure could throw the baby out with the bath water. There's a very fine line. The services that data brokers provide help make business more efficient, they keep costs low for all Americans across a wide range of services, from mortgage rates to online shopping and a wide range of financial services. So, we need to make sure that we preserve the positive uses of this data, as well.

And, of course, I look forward to working with you and the rest— and the balance of the Members of this Committee, because it is timely, it is necessary, and we've got to do it right.

Thank you.

Senator SMITH. Thank you, Senator Burns.

Senator Nelson?

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator BILL NELSON. Mr. Chairman, thank you for holding this hearing, and thank you for your personal interest.

One of the bills that is in front of us, Mr. Chairman, is the bill that Senator Schumer and I have filed. The hearing is timely, because we just had another example of missing records, to the tune of 3.9 million records. We don't know if it's identity theft, but it's certainly subject to identity theft, because they are now missing. And if you add up all of the records that have been lost, missing, or stolen, starting back with ChoicePoint, which is the Georgia company that first came to light because of a California law that said that the people whose records were missing had to be notified—that was just a few months ago—in that short period of time, 8.8 million people's records are missing.

Now, if this isn't an eye-opening threat to Americans' privacy, then I don't know what is. And it's not only the individual threats and how to go about getting your identity back that Senator Schumer and I address in this legislation, but look at the national security implications, look at what a terrorist can do, in trying to steal someone's identity. And, if that's not enough, look at the threat to electronic commerce. Consumers are losing trust in our system of electronic commerce, especially when they learn about these huge unsecured data warehouses, and suddenly their information is missing. And now you will find that identity theft is the number-one skyrocketing consumer fraud.

So, I believe, Mr. Chairman, that the Congress needs to act now. That's the timely manner. And I want to thank you again for holding this hearing.

Senator SMITH. Thank you, Senator Nelson. We look forward to sharing ideas with you on how to make a good bill better, if we can.

And, in that spirit, we welcome our colleague, Senator Schumer here, and we'll ask you to go first, and then my fellow statesman, Congresswoman Darlene Hooley.

Senator Schumer?

STATEMENT OF HON. CHARLES E. SCHUMER, U.S. SENATOR FROM NEW YORK

Senator SCHUMER. Well, thank you, Mr. Chairman. I want to thank you, Chairman Stevens, and Ranking Member Inouye for having this hearing, and more importantly is the general interest that this Committee has shown in this very important issue.

I'd like to commend my colleague, Senator Feinstein, who I believe will be coming——

Senator SMITH. She has just arrived.

Senator SCHUMER.—as well. Oh.

Senator SMITH. Welcome, Senator Feinstein.

Senator SCHUMER. See, I didn't even know you were in the room.

Senator SMITH. I'm very pleased she got the memo about—this is Seersucker day.

Senator FEINSTEIN. Yes.

Senator SMITH. So, I'm not the only one looking like an ice cream salesman here.

[Laughter.]

Senator SCHUMER. Well, I'd like to comment on my National Seersucker Day Resolution that——

[Laughter.]

Senator SCHUMER. Anyway, I want to thank you, and I want to thank Senator Feinstein for her leadership on this issue, as well.

Identity theft is just everywhere. And the number of people who call every one of our offices for advice, just to express their outrage, is growing and growing and growing. It's, of course, natural. Technology has allowed us to transfer information quickly, and, Senator Burns is right, it's an important part of the economy, and we don't want to stop it. But, at the same time, given all the new technology, it makes information about people, which used to be just proprietary—it makes it valuable. These days, information about people is as valuable as gold, and it ought to be treated that way. We don't transport gold the way we transport a crate of oranges, and we shouldn't transport people's identities, people's information, the way we transport a crate of oranges. We don't store it the same way. We have Fort Knox. Well, we ought to store this information in a different way.

The bottom line is very simple, Mr. Chairman. What bank robbery was to the Depression Era, identity theft is to the Information Age. But, in a sense, identity thieves are even worse than bank robbers, because they not only steal your money, they steal your time, your sense of security, and your peace of mind. That's what the thieves, the identity thieves, do. And unless Congress, companies, and consumers take action, this is an epidemic that threatens to spiral out of control.

Senator Nelson and I believe that Congressional action must be quick, but it also must be comprehensive. If you plug one part of the loophole, the identity thieves are going to find another way to do it. That's what the technology allows them to do, all this—all of us, in the Information Age. And I'm glad to say that identity theft is not a partisan issue—it's not a Democratic issue, a Republican issue—it's a nonpartisan consumer and economic crisis, and there's no excuse for Congress failing to act in a bipartisan way.

The legislation that Senator Nelson and I have introduced offers a truly comprehensive solution. Instead of just adding another square to the current patchwork quilt of regulations, our bill provides a real security blanket for the American consumer. To really tackle identity theft, our bill takes an aggressive approach in three areas.

One, empowering consumers. The average consumer, it's estimated—by the FTC—who's a victim of identify theft, spends 175 hours restoring their credit information and their credit integrity. That is more than four 40-hour workweeks. So, people, who are busy with their jobs, with their families, with life's joys and life's trials, have to then take a huge amount of time to try and restore their good name back, even though they did nothing wrong. So, we empower consumers, and give them more rights there.

Second, we protect our most personal information. We say, to people who carry this information, "You have a new special responsibility. You can't just say, "Well, it wasn't my fault; we were just doing what we did years ago." What they did 10 years ago was not good enough 5 years ago, and what they did 5 years ago is not good enough for today.

And, finally, what we do is, we try to make sure that consumers are empowered. And let me describe that. We make companies, of course, tell consumers when their information has been breached. We also require companies to tell them if the company plans to sell sensitive personal information they collect. So, consumers can make intelligent decisions about whom to trust. When you buy something, if somebody's going to use all your information, you should have a right to say, "I don't want to buy it here. I want to go somewhere else, where they won't sell the information about me." We protect the information.

We believe an ounce of prevention is worth a pound of cure. And our bill makes prevention a centerpiece of the effort against identity theft. We establish procedures for the FTC to require companies to authenticate those who try to buy sensitive personal information from them, to stop situations where companies like ChoicePoint, for example, sell their personal information to identity-theft rings posing as legitimate businesses.

We also insist that every company that stores sensitive information take reasonable steps to protect it, a simple minimum requirement. The Federal Trade Commission recently applauded this provision because of its potential, in their words, to reduce the risk of identity theft.

All companies who keep sensitive personal information need to take responsibility. They need to guard our identities as if they were gold, because, in the hands of identity thieves, they are gold.

We also intend—we are now adding an additional provision to our bill to deal with the transportation or storage of sensitive personal information. What we've learned from what happened at Citigroup is that we need standards when that information is transported. You can't just treat it like you're transporting any good, because it's too valuable, it's too important; and, therefore, we require standards, in terms of transportation, depending on how much information and how valuable it is, and we also encourage encryption, so that, even if it's stolen, this identity thief is not able to use it.

Right now, we have a better chance of tracking down a lost book from Amazon than some banks have had in tracking down millions of sensitive records lost in transit. That has to stop.

And, finally, helping victims. Our bill tries to provide relief to the millions of Americans each year who fall victim to identity theft. We create an Office of Identity Theft, within the FTC, which will serve as a one-stop shop. When a consumer's identity is stolen, they can call and say, "Help me. How do I deal with all the various things that I have to deal with because of that?"

So, Mr. Chairman, I encourage every company in America, and especially in my State of New York, to do a top-to-bottom review of its procedures for handling consumers' sensitive personal information to stave off more incidents where information is exposed. We can—companies can do that even before any legislation passes, and help their customers and help themselves.

In conclusion, Mr. Chairman—I see the yellow light is on—identity theft is a serious issue that deserves real comprehensive action. I hope this Committee will give the Schumer-Nelson bill the consideration that we believe it deserves.

Thank you for your interest and the opportunity to testify. And I apologize, I'll have to excuse myself, because—they're buzzing me—we have a—I need to make a quorum in the Judiciary Committee.

Senator SMITH. Why don't you stick around?

[Laughter.]

Senator SCHUMER. I'll come back.

[Laughter.]

Senator FEINSTEIN. Ulterior motive.

[Laughter.]

Senator SMITH. No, we understand, Senator Schumer.

Senator SCHUMER. It's to make a quorum. That's good for you.

Senator SMITH. Oh, OK. OK.

[Laughter.]

Senator SCHUMER. How I vote may not be, but my quorum presence is.

[Laughter.]

Senator SMITH. Senator Feinstein, I had announced Congresswoman Hooley, but does your schedule permit——

Senator FEINSTEIN. If there—I, also, am on Judiciary. If he makes the quorum——

Senator SMITH. Is that all right——

Senator FEINSTEIN.—I will stay——

Senator SMITH.—with you, Congresswoman Hooley?

Senator FEINSTEIN.—for a while.

Senator SMITH. Thank you.

Senator Feinstein?

Senator FEINSTEIN. Thank you.

For me? All right, thank you.

STATEMENT OF HON. DIANNE FEINSTEIN, U.S. SENATOR FROM CALIFORNIA

Senator FEINSTEIN. I'm—can't see over the table. This is a first for me. I'm tall, but this chair—if you don't mind, I'll just move one.

Mr. Chairman, I—and Ranking Member Inouye and Members on both sides—I've been working on this issue for over 3 years now. It has to do, really, with privacy. And I think most people don't understand——

Senator BURNS. Senator, could you pull that up so everybody can hear?

Senator FEINSTEIN. Sorry. I think—my low voice? Yes. I think most people don't understand that virtually everything they buy, do—when they buy from a catalog, when they buy insurance, when they buy a car, when they mortgage a home, when they get a loan—that all of that data is collated, and it has become big business. It's sold by banks to their affiliates. Citibank, I believe, sells to thousands of different businesses, all this data. And its database companies have developed programs which compile this data and then sell it out.

Well, identity theft has become the largest-growing crime in America, with ten million victims. It's bigger than all of the theft and burglary in history was, in terms of loss. And nobody knows that their identity has been compromised.

I've presented three bills. One is a notification bill, which is in Judiciary, and I'd like to have you take a look at it. Essentially, it says that when a database is breached, the data company must, within a reasonable period of time, alert the consumer that their data has been breached and tell them how to take the necessary steps to keep their credit intact.

Notification is really important. Over the past 2 years, there have been 34 major data breaches. Just this morning, the FDIC, the second Federal agency, had its database breached, with people illegally, now, joining credit bureaus with data from that breach.

Over the past 2 years, approximately 18,393,180 people in this country have been exposed or affected by identity theft. Last year, the total cost to individuals and businesses from this theft, believe it or not, was $52.6 billion. It is huge.

Let me give you a few examples. CitiFinancial, earlier this month, announced that a box of computer tapes with unencrypted account information for 3.9 million customers had been lost in shipment. Look at the value of that loss. Somebody picks it up, they can go to Paris and sit there and assume other people's identities. They can be in Chicago and rip somebody off in San Diego. It is an insidious kind of opening.

The Bank of America announced they lost tapes containing 1.2 million Federal employees. ChoicePoint, 145,000. Both the California and Colorado Departments of Health had laptops stolen, which jeopardized personal information of 25,000 residents. And the list goes on and on. DSW, LexisNexis, the University of California system, Boston College, HSBC, Ameritrade, Department of Justice, and now FDIC.

California, in 2003, was the first state to require notification in the event of a data breach. Now, I believe that that bill is really responsible for the notice that's now being given throughout the United States, and that if it had not been for the California law, we may well not be privy to all of the breaches we are aware of today. So, California began a trend, and we're now seeing other states seeing the notification—the necessity of notification laws.

At present, the states are out ahead of the Congress. States like Arkansas, Georgia, Indiana, Montana, North Dakota, and Washington State are moving. Now, this creates problems, because different states are going to have different laws.

Now, earlier this year I introduced a second version of my earlier bill—and we're still working on it—and this would require the Federal Government or a business notify individuals when there has been a breach that involves Social Security numbers, driver's licenses, or state identification numbers, and financial account information. The bill would require that notice be sent out, without unreasonable delay, by mail or e-mail. It would allow for exceptions to notice for law enforcement and national security purposes. It would impose civil penalties for failures to notify, such as $1,000 per individual whose personal data was compromised, or not more than $50,000 per day while the failure to notify continues. It would allow individuals to place an extended fraud alert on their credit report to protect themselves. And it would allow state attorneys general to protect the interests of residents in their state when the Federal Government or businesses fail to notify individuals of a breach.

Now, there are some contentious issues that I've found that I want to make you aware of.

The first is the issue of preemption, whether preemption should be a floor or a ceiling. The consumer groups believe that the states should have the right to enter this area, as well. And that comes directly into conflict with the concept of one uniform law all across the United States. We're trying to work that out.

Second, exactly what triggers notice to be given to individuals, and striking a balance between over-notification and inadequate notice in dealing with companies—that has become a problem.

And, finally, whether alternative notification procedures or so-called safe-harbor provisions—the California bill had a safe-harbor provision. Consumer groups do not like a safe-harbor provision. Businesses will adamantly oppose anything without a safe-harbor provision. So, we are trying to work out a safe-harbor provision that protects individuals against identity theft in certain situations.

We also have a bill that would do something on the privacy issue. Senator Schumer spoke of it. I mean, consider this. Our Social Security number and driver's license are the two major breeder documents that are there. Falling into the wrong hands, they allow people all kinds of access. In the wrong hands, that's fraudulent access; but, nonetheless, it happens. Personal financial data and personal health data, I think, used for commercial purposes without the individual's assent or even knowledge, I believe, is wrong.

Now, California passed a law having to do with this. The banks and insurance companies supported it. Then when I tried to do it here, the same law, they came back and opposed it, and killed it.

So, we're fighting, in this whole arena, big interests out there who make a lot of money on these databases and don't want the public to receive a notice that says, "We sell your data, as indicated here. May we have your permission to do so, yes or no?" They don't want to do that. So, that is a significant issue as identity theft reaches epic proportions.

And the last point, and the last bill that we've worked on now for 5 years, and it would seem so simple—it has gone to Finance, it runs into trouble with Finance staff—and that is protection through the redaction of Social Security numbers on public documents. And, also, both of these documents, driver's license and Social Security, being sold through the Internet, where you can buy somebody's number for $12 or $15.

These are huge questions that this new Internet technology, as well as database technology, presents to the Congress. I think, because of the excruciating pain caused, in terms of the loss of identity to so many people, the inordinate cost of this, that Congress really has a major issue before it.

So, I'd like to just put into your record, if I might, my three bills on the subject that you could take a look at and, obviously, do with what you wish.

Senator SMITH. We'll receive those without objection, and we appreciate so much your concern about the issue, Senator Feinstein.

A point of clarification for me, and perhaps my colleagues. In your view, why did the banks support the legislation in California, but oppose it nationally?

Senator FEINSTEIN. I've had conversations with CEOs on this subject. And one of the things, banks are buying more industries, and they want to be able to share this information with those industries. So, there is a question of liaison, there is a question of transmitting data within those industries. Now, what happens is, with—you have data breaches which is happening. This is exposing literally tens of millions of people. And it's all without their knowledge. So, this has added an additional dimension.

The bill that I'm speaking of, that you just asked about, Senator Smith, actually was before we knew about these database breaches. The database breaches, I think, gives more momentum to my— we'll see, because there are powerful interests.

Senator SMITH. Well, thank you for your interest in this very important legislation, and we'll look forward to working with the ideas in your bill, and perhaps ultimately incorporating many, or most, into a Committee bill.

Senator FEINSTEIN. Thanks very much, I appreciate it.

Senator SMITH. Thank you.

Senator FEINSTEIN. Thank you.

Senator SMITH. Congresswoman Hooley, the mike is yours.

STATEMENT OF HON. DARLENE HOOLEY, U.S. REPRESENTATIVE FROM OREGON

Ms. HOOLEY. Thank you, Chairman Smith. And I really appreciate the opportunity to testify in front of you. Thanks to all the Committee Members and Ranking Member Inouye.

I am one of millions of former credit-card fraud victims and a Member of the House Financial Services Committee, and I've had a long interest in protecting consumers from potential identity theft. I'm delighted that you're working on this, that you're going to introduce a bill on this, and I hope it is as comprehensive as you can make it.

When I started on this issue about 6 years ago, there were thousands of victims of identity theft. Today, there are over ten million victims of identity theft, and it is growing. This is a way to steal your money without putting a gun to your head. They can do it over the Internet and through computers. It represents a fundamental threat to our e-commerce, to our overall economy and, frankly, to our homeland security. We are no longer facing just hobby hackers; these are skilled criminals. ID theft is big business. It is imperative that Congress and the private sector work together to make certain that sensitive personal information is protected.

Congress, last year, with the passage of the FACT Act, provided landmark consumer protections, including free annual access to credit reports. We know that if people know what's on their credit report, they will take some responsibility to make sure that credit report is accurate. We have to build on that success.

We all know that there were recent high-profile data-security breaches. You've heard all about them from the other two Members. And what that does is undermine the public confidence in the data-security practices of U.S. companies that have exposed millions of consumers to potential fraud and identity theft. Theft of thousands of consumer files from companies like ChoicePoint and LexisNexis illustrate how broadly our private information is collected and sold without our knowledge or consent, and how vulnerable these private databases are to both traditional and high-tech forms of theft.

There are many consumers who think, "Oh, I've kept tight control over my personal and financial information," but they can still be a victim of identity theft, because companies that seek to profit from their personal information may have inadequate security standards, or businesses may fall victims to criminal activities.

With respect to data breaches, there are immediate steps. First of all, data brokers should be required to operate by the same information-sharing standards and consumer protections as consumer-reporting agencies. Because credit reports contain confidential personal information, the Fair Credit Report Act only allows an individual's credit report to be released to certain people for clearly defined purposes. FCRA requires that consumer-reporting agencies certify the purpose for which the report is being obtained, and that that report will not be used for any other purpose. Despite harboring similar sensitive personal information, data brokers currently face no such restrictions.

Second, Congress should impose data-security obligations and standards on data brokers and consumer-reporting agencies as the

Gramm-Leach-Bliley Act requires of regulated financial institutions.

Third, Congress should establish uniform requirements for data brokers, consumer-reporting agencies, and financial institutions to notify consumers. And, again, I think, in all of your bills, there are notification procedures, and that has to be a balance. Congress should include in such a notice the date of the breach, specific information that was acquired, the actions being taken by the consumer-reporting agencies, financial institution, or data broker, an explanation of how a consumer may obtain a copy of their consumer report free of charge, and how they may place fraud alert on their consumer reports to discourage unauthorized use, and a toll-free number where consumers can obtain additional information about the security breach and their options to protect their consumer file.

Finally, Congress must place greater responsibility on retail merchants to protect their customer payment account information.

By accomplishing these initial goals, Congress will provide consumers with the protections they deserve, and provide the clarity and uniformity that industry needs in order to service their customers.

In addition, there are a whole host of identity-theft proposals that I think warrant further examination and vigorous debate, and I'm just going to go through a very quick list. One, people have talked about—I think it needs to be examined—an Office of ID Theft Czar at the FTC, or elsewhere. You need more money in the Department of Justice and Secret Service to investigate and prosecute perpetrators of mass ID fraud. I think you need to allow consumers to protect their consumer file with optional credit freezes, encourage industry and consumer use of a second-factor authentication, effective Federal legislation to combat the practice of phishing and pharming—and that's with a "p," and not an "f"—explore effective biometric technology; and, last, but not least, I think you have to seriously look at methamphetamine. There is an incredibly close alliance between meth use and ID theft. And if you don't go on the track of trying to stop methamphetamines, it will only help identity theft grow.

Thank you again, very much, for this opportunity to testify in front of the Committee.

Senator SMITH. Thank you very much, Darlene. And I want to highlight—what you just said as your last point, and that is the linkage between methamphetamines and identity theft. Many of the crimes that are committed by methamphetamine users relate to identity theft because of the kinds of resources and information that they are able to glean from this practice. So, it has an implication well beyond just someone's finances. Sometimes they're being put in touch without their notice or knowledge, with some pretty shady characters peddling one of the worst of the drugs in our society, that is truly becoming a plague across our whole country.

Thank you very much.

Ms. HOOLEY. You're welcome. Thank you.

Senator SMITH. Appreciate your being here.

I have been asked by several Members of the Committee to allow Mr. Sorrell, the President of the National Association of Attorneys

General, to testify very briefly, before the FTC, because his statement is short and the Committee has a few questions for him. The normal protocol is for the FTC to testify first, but I'm asking for the indulgence of the Committee to allow this to occur.

So, Mr. Sorrell, if you will come forward, we'll receive your testimony.

STATEMENT OF HON. WILLIAM H. SORRELL, VERMONT ATTORNEY GENERAL; PRESIDENT, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

Mr. SORRELL. Thank you, Senator Smith, members of the Committee. I appreciate your giving me the opportunity to appear before you today to speak on these important issues.

I am currently the President of the National Association of Attorneys General, but I have not consulted with all of my colleagues about the substance of my testimony. I'm confident that most, if not all, would agree with the sentiments that I will express today, and have expressed in my prepared, or filed, testimony. But please let me testify as the Attorney General of Vermont today.

Senator SMITH. Thank you. You're welcome.

Mr. SORRELL. And I assume, Senator, that my pre-filed testimony will be made part of the record.

Senator SMITH. We'll include it in the record, if there's no objection. Hearing none, so ordered.

Mr. SORRELL. And if you'd allow me, Senator, I didn't know that Seersucker suits were allowed attire today, and—I have one, and I don't find many opportunities in Vermont to wear it, so I'm sorry I didn't get that information.

[Laughter.]

Senator SMITH. We've adopted it, above the Mason-Dixon Line, at the urging of our southern colleagues.

[Laughter.]

Senator SMITH. And thank you, Senator Nelson, for wearing yours today.

[Laughter.]

Senator SMITH. And Senator Snowe, from Maine, absolutely.

Mr. SORRELL. As our culture changes, the way we go about our commerce changes, not only for legitimate businesses, but those scam-artists and thieves who, maybe in the past, broke into our homes to steal our jewelry, our televisions, our computers, our stereos, or whatever. But the reality is—and we, as individuals, we lock our doors, we lock our cars, we park in well-lit areas, we try to protect ourselves—but the reality is that, quite apart from our cash assets and other valuables—is that, as our economy has changed, our truly valuable assets are frequently not our possessions, but our access to credit. And we can't lock our doors in the same way to protect ourselves from those who want to access our credit or to, in this information and electronic age, to withdraw the assets that we have with financial institutions. And, frankly, consumers need government help to allow us to figuratively lock our doors and protect ourselves from identity theft. We've heard the earlier testimony today—I'm sure we'll hear more from the Commission—about, you know, ten million Americans victimized by identity theft, the number of hours that it takes to try to regain your good name when you're the victim of identity theft. And, you know, it's like the crime that keeps victimizing you. As you try to access credit after someone has assumed your identity, and scammed either you individually or businesses to the tune of $50 billion a year in a crime that is continuing to escalate.

And so, we do need government assistance to protect our personal information. And I think we all owe a debt of gratitude to the legislators of California for enacting their security-breach notification law. But for the existence of the law—I don't think we would be focused as much today as we are, but for the California law and the ChoicePoint and then the subsequent disclosures, which seem to be escalating in numbers and volume of records and individuals affected. It's almost a daily, certainly a weekly, occurrence of new security breaches coming to the fore.

The states have followed California's lead. And a handful of states have passed their own security-breach laws. Many other state legislators are considering doing the same. We believe, and strongly encourage, that there be a Federal security-breach notification law. At the same time, we remain concerned that what is done federally remain a floor, and not a ceiling. Similar to what you did with the Gramm-Leach-Bliley legislation, several years back, where you adopted a national opt-out standard for financial institutions, banks, insurance companies to traffic in our personal information, you allowed states, if they wished, to go further. Vermont was one of the states that took advantage of your lack of preemption; and so, a more protective standard of opt-in standard is the law in Vermont. And for those who feel that there has to be one standard, we can't have these patchwork quilt—a quilt of regulations—the Vermont economy has not suffered. Banks, financial institutions, and insurance companies have continued to come into Vermont since the more protective opt-in standard has been implemented. So, we ask for a Federal law, notification law, a floor, not a ceiling.

Similarly, we ask you to enact a Federal unified, one-place program to regulate data brokers. Again, that is a floor, and not a ceiling. We ask you to strengthen the so-called safeguard rules under Gramm-Leach-Bliley to require definitive minimum standards—minimum standards—for information security and ensure that these rules are written broadly enough to cover data brokers. And, finally, we just ask you to recognize the important role of state legislatures and state regulators and enforcement authorities in the development of laws in this area of security breaches and security freeze legislation.

[The prepared statement of Mr. Sorrell follows:]

PREPARED STATEMENT OF WILLIAM H. SORRELL, VERMONT ATTORNEY GENERAL; PRESIDENT, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

I. Introduction

Chairman Stevens, Co-Chairman Inouye, and honorable Members of the Committee, I am William H. Sorrell, Attorney General of the State of Vermont and President of the National Association of Attorneys General. I very much appreciate the opportunity to appear before you today to discuss security breaches relating to personal information of consumers and to discuss my recommendations for addressing some of the problems in this area.

The public has become aware of numerous incidences of security breaches in the past 2 months as a result of California's innovative security breach notification laws. These security breaches expose millions of consumers to potential identity theft, a serious and rapidly growing crime that now costs our Nation $50 billion per year. I make the following recommendations to address the problems of security breaches:

- Enact a Federal security breach notification law that doesn't preempt more-protective state laws.
- Enact a unified Federal program for regulation of data brokers that doesn't preempt more-protective state laws.
- Strengthen the Gramm-Leach-Bliley "Safeguards Rules" to require definitive minimum standards for information security, and ensure that these rules cover data brokers.
- Recognize the important role of state legislative and law enforcement efforts, particularly in developing security freeze laws.

II. The Growth of Security Breaches

Over the past several months, consumers, law enforcement officials, and policymakers have learned about a rising incidence of security breaches at private companies and public institutions that have exposed consumers' personal information to unauthorized third parties. Separately, these breaches involve the personal information in tens of thousands, hundreds of thousands, and even millions of records about consumers nationwide.

A. Numerous Serious Incidences of Security Breaches Have Occurred Since 2002

Nine known incidences of serious security breaches have occurred in the past few years. It is instructive to examine each one in some detail.

- *Ford Motor Credit:* In 2002, three individuals were arrested for downloading credit reports on more than 30,000 consumers, and then selling the credit reports to street criminals who emptied the victims' bank accounts and opened credit cards in their names. The scheme centered on an employee of Teledata, a company that provides credit reports to banks and other lenders. The employee stole the passwords and codes of Teledata clients, such as Ford Motor Company, in order to download credit reports from the three major credit reporting agencies. Over a 10-month period, the password and code for Ford Motor Credit alone was used to download 13,000 credit reports from just one credit reporting agency, Experian. Losses were originally calculated at $2.7 million, but were expected to rise significantly in the weeks after the arrest.[1]
- *Acxiom:* In 2003, the records of an unknown number of consumers were stolen from Acxiom, a commercial data broker based in Little Rock, Arkansas. Hackers were able to download the passwords of 300 business accounts on Acxiom's system, costing the company $5.8 million in losses.[2]
- *ChoicePoint:* In February 2005, ChoicePoint notified 144,000 consumers nationwide that their personal data may have been accessed by "unauthorized third parties" posing as small-business customers. ChoicePoint, an Atlanta-based data broker and specialty credit reporting agency with databases that contain 19 billion public records about consumers and businesses, reported that identity thieves created as many as 50 fake companies that posed as customers and gained access to consumer data.[3] The Los Angeles, California, Sheriff's Department estimates that the number of consumers whose personal data has been compromised is in the millions.[4]
- Bank of America: Also in February 2005, Bank of America announced that it lost computer back-up tapes containing personal information, including names and Social Security numbers (SSNs), relating to 1.2 million Federal workers. The tapes had been lost 2 months earlier in December 2004. Bank of America received permission from its Federal regulators to notify consumers about the security problem in mid-February.[5]
- *DSW Shoe Warehouse:* On March 8, 2005, DSW Shoe Warehouse announced the theft of credit card information, including account numbers and customer names, relating to customers at more than 100 of its 175 stores. The theft took place over a three-month period beginning in early December 2004. The theft was originally reported to affect "more than 100,000" consumers. On April 18, 2005, DSW disclosed that the number of affected consumers was 1.4 million, 10 times as many as originally reported. DSW is a subsidiary of Retail Ventures, Inc., based in Columbus, Ohio.[6]

- *LexisNexis:* On March 10, 2005, LexisNexis owner Reed Elsevier PLC announced that records of about 32,000 consumers were accessed and compromised when intruders used log-ins and passwords of a few legitimate customers to obtain access to a database of public records. The records included names, addresses, SSNs, and driver's license numbers. The breach occurred at Boca Raton, Florida-based Seisint, a data broker recently purchased by Reed Elsevier and integrated into LexisNexis. Seisint stores millions of personal records about consumers nationwide.[7] On April 12, 2005, LexisNexis announced that an additional 280,000 consumers nationwide had been affected by other security breaches of Seisint data over the past 2 years.[8]
- *Boston College:* In late March 2005, Boston College notified 106,000 alumni that a hacker had gained access to a computer database containing their personal information. College officials stated that they had to tell the affected alumni living in California about the theft due to California's notification law. The officials therefore decided to tell alumni who live in other states, too, to help them limit their exposure to identity theft.[9]
- *University of California:* On April 1, 2005, University of California-Berkeley officials announced that a laptop computer containing information about 98,000 students and alumni had been stolen a month earlier. The information, including names, SSNs, and in some instances birth dates and addresses, was unencrypted, although the laptop was password-protected. This breach followed another incident at UC-Berkeley in September 2004 in which a hacker obtained the names, SSNs, and other identifying information belonging to 600,000 people.[10]
- *San Jose Medical Group:* On April 8, 2005, the San Jose (California) Medical Group notified nearly 185,000 current and former patients that their financial and medical records might have been exposed following the theft of computers. The theft occurred after the group copied patient and financial information from its secure servers to two local PCs as part of a patient billing project and the group's year-end audit.[11]
- *Ameritrade:* On April 19, 2005, Ameritrade reported that account information relating to as many as 200,000 customers may have been lost when a package containing tapes with back-up information on customers' accounts went missing. A shipping company Ameritrade uses misplaced the tapes.[12]
- *HSBC/Ralph Lauren:* On April 13, 2005, the British financial firm HSBC announced that criminals may have obtained access to credit card information of at least 180,000 consumers who used MasterCard credit cards to make purchases at Polo Ralph Lauren Corp. The circumstances that led to the breach have remained murky. Although the letter sent by HSBC told affected consumers that the financial firm was "unaware of any fraudulent activity on your account," HSBC advised consumers to replace their credit cards.[13]
- *Time Warner:* On May 3, 2005, Time Warner announced that a cooler-sized container of computer tapes containing personal information about 600,000 current and former employees was lost by data-storage company Iron Mountain, Inc., based in Boston, apparently during a truck ride to a data-storage facility. The lost tapes contained the names and SSNs, as well as other data, about 85,000 current and over 500,000 former employees dating to 1986.[14]
- *Bank of America, Commerce Bank, PNC Bank, and Wachovia:* On May 23, 2005, Hackensack, New Jersey, police announced that bank employees may have stolen financial records of 700,000 customers of four banks: Charlotte, North Carolina-based Bank of America and Wachovia, Cherry Hill, New Jersey-based Commerce Bank, and PNC Bank of Pittsburgh. The bank employees sold the financial records to collection agencies, according to the police.[15]
- *CitiFinancial:* On June 6, 2005, CitiFinancial, the consumer finance division of Citigroup, Inc., said that computer tapes containing personal data relating to 3.9 million U.S. customers had been lost by shipper UPS. The data included account information, payment histories, and SSNs.[16]

Several conclusions can be drawn from a review of these events. Hackers and identity thieves employ both high-tech means for stealing passwords and other log-in information to access consumers' personal information, as evidenced by the LexisNexis and Acxiom breaches, as well as low-tech techniques to breach information systems, as evidenced by the ChoicePoint incident. Other security breaches, such as those experienced by CitiFinancial, Time Warner, and HSBC, reveal gaps in offline handling of personal information, including trucking, air transport, and other traditional logistical systems. In addition, although the pace of disclosures about these breaches has accelerated over the past few months, it is safe to presume that breaches have been occurring regularly over the past several years. What has changed is not the existence of the problem, but rather the public's awareness of it.

B. The Public Has Learned About These Breaches As a Result of California's Security Breach Notification Laws

On July 1, 2003, California's security breach notification laws went into effect. These laws require businesses and California public institutions to notify the public about any breach of the security of their computer information system where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[17] California's laws require that the notice be given without unreasonable delay and consistent with the legitimate needs of law enforcement, who can request a delay in notification if the notice would impede a criminal investigation of the incidence.[18] "Personal Information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data element is not encrypted:

- Social Security number.
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[19]

The California law allows a business or public institution to satisfy the notice requirement in several ways: written notice through the mail; electronic notice in conformity with the Federal Electronic Signatures Act;[20] substitute notice through e-mail, website publication, and major statewide news media if more than 500,000 consumers are affected; or in conformity with the business's or institution's own notification system, if it meets the timeliness requirements of the California security breach notification laws.[21]

California's unique and innovative laws in this area have ensured awareness of the growing problem of data leaks that are plaguing our Nation's businesses and public institutions.

III. The Effect of Security Breaches

Identity theft, already a growing problem, is likely to grow even more rapidly as a result of security breaches. These data leaks expose consumers to the threat of identity theft by the criminals who gain access to consumers' personal information. MSNBC has noted that in the six-week period from mid-February through early April, the rash of data heists has exposed more than two million U.S. consumers to possible identity theft.[22] Since that time, an additional 4.6 million U.S. consumers and employees have been exposed to possible identity theft, bringing the total number of consumers affected by data heists in 2005 to 6.6 million U.S. consumers and employees.

Current estimates of the incidence of identity theft in the United States are disturbingly high. According to a survey released in January 2005 by Javelin Strategy & Research, about 9.3 million U.S. adults were victims of identity theft between October 2003 and September 2004.[23]

Even though the vast majority of victims of identity theft do not report the crime to law enforcement authorities or credit bureaus,[24] the reported incidence of identity theft has grown dramatically. The Federal Trade Commission reported in February 2005 that the number of identity theft complaints submitted to its Consumer Sentinel database has grown from 161,896 in 2002 to 246,570 in 2004,[25] representing a growth rate of more than 50 percent in 2 years. Victims' information is misused to perpetrate financial fraud in the vast majority of cases: fraud involving credit cards, checking and savings accounts, and electronic funds transfers represented 46 percent of the complaints in 2004.[26] Out of the 50 Metropolitan Statistical Areas that have generated the greatest number of complaints relative to population, six are in California, four are in Texas, three each in of New York, Ohio, Pennsylvania, and Wisconsin, and two are in Illinois.[27] Arizona victims of identity theft have filed the largest number of complaints relative to population, followed by Nevada, California, Texas, Colorado, Florida, New York, Washington, Oregon, and Illinois.[28]

Identity theft has a deeply negative impact on our Nation's economy. According to a survey published by the Federal Trade Commission in September 2003, the total cost of identity theft approaches $50 billion per year, with victims bearing about $5 billion of the losses and businesses bearing the remaining $45 billion.[29] The average loss from the misuse of a victim's personal information is $4,800, but for victims who had new credit card and other accounts opened in their name, the average loss is $10,200.[30] Overall, victims spent almost 300 million hours resolving problems relating to identity theft in 1 year, with almost two-thirds of this time—194 million hours—spent by victims who had new credit card and other accounts opened in their name.[31]

IV. Consumers' and State Officials' Concerns about Security Breaches

The recent rash of information heists has had several important effects on the state and local level. Consumers have expressed concern about their current level of knowledge of security breaches and what they realistically can do if they become a victim. State Attorneys General and other state and local officials have taken action in a number of areas to resolve these concerns.

A. Consumers Across the Nation Want to Receive Notice of Security Breaches

The citizens of California have received notice of security breaches as a result of their state's innovative law. Consumers in the remaining 49 states, the District of Columbia, and the territories want the same right to receive notice when their personal information is accessed in an unauthorized manner. Unfortunately, in the absence of other state laws or a Federal minimum standard, consumers in the other states have not consistently received notices in the recent spate of incidences. LexisNexis sent notices on a voluntary basis to affected consumers nationwide. ChoicePoint originally sent notices only to California residents; only after receiving letters from the Attorneys General of numerous states did ChoicePoint expand its notification process to include potentially affected consumers in all states.[32] The Ohio Attorney General was forced to file suit against DSW, Inc., because the company had not provided individual notice to half of the consumers—approximately 700,000 out of 1.4 million—affected by the security breach it experienced.[33]

In addition to haphazard notification, the paucity of regulation in this area has led to another problem. The notices that were actually received by consumers came in envelopes from "ChoicePoint." Consumers have no idea who ChoicePoint is because consumers typically have no business relationship with ChoicePoint. We learned of instances where consumers tossed out the notification letters without opening them, on the assumption that the letters were another unsolicited offer for a credit card or some other piece of junk mail.

Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by identity theft. The Federal Trade Commission reports that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly.[34] For example, when the misuse was discovered within 5 months of its onset, the value of the damage was less than $5,000 in 82 percent of the cases. When victims did not discover the misuse for 6 months or more, the value of the damage was $5,000 or more in 44 percent of the cases. In addition, new accounts were opened in less than 10 percent of the cases when it took victims less than a month to discover that their information was being misused, while new accounts were opened in 45 percent of cases when 6 months or more elapsed before the misuse was discovered.[35]

To ensure that citizens across the Nation receive adequate notice about security breaches, this past spring 28 states considered legislation modeled on California's law.[36] As of today, six states—Arkansas, Georgia, Indiana, Montana, North Dakota, and Washington State—enacted security breach notification laws this session.[37] Legislatures in two additional states—Illinois and North Carolina—have passed security breach notification bills, but these bills have not yet been signed into law.

B. After Learning About a Breach of Their Personal Information, Consumers Want to Review Their Credit Reports to Determine if They Are Victims of Identity Theft

The 2003 amendments to the Federal Fair Credit Reporting Act[38] gave consumers the right to receive a free copy of their credit report once every 12 months, following the example previously set by 7 states that require credit reporting agencies to provide free reports to their citizens.[39] However, because the FTC allowed the nationwide credit reporting agencies to stagger the implementation of the national free credit report, consumers in the Southern states—Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas—were not able to order their free reports under Federal law until June 1, 2005. And consumers in the Eastern states—Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Vermont, Virginia, and West Virginia, as well as the District of Columbia, Puerto Rico, and all U.S. territories—are not able to order their free reports under Federal law until September 1, 2005.[40] As a result, many citizens have been unable to see their credit report for free during this time of heightened anxiety over possible identity theft, causing great frustration in the Eastern and Southern states.

In addition, in those Eastern and Southern states—like Vermont—that already require credit reporting agencies to provide free credit reports under *state* law, consumers have been confused and frustrated because the credit reporting agencies have not adequately adjusted their systems to enable consumers in these states to easily access their free report under *state* law. Many consumers in Vermont attempted to obtain their free report under Vermont law after learning about the ChoicePoint and other security breaches, only to be told—incorrectly—by the credit bureaus' voice-mail systems that they were not eligible for a free credit report.

C. Consumers Want to Control Access to Their Credit Reports so That Identity Theft does not Occur

The 2003 amendments to the Federal Fair Credit Reporting Act also gave consumers the right to place a "fraud alert" on their credit reports for at least 90 days, with extended alerts lasting for up to 7 years in cases where identity theft occurs.[41] Yet many states are considering enacting stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches.[42] Two states, California and Texas, allow consumers to place a "security freeze" on their credit report. A security freeze allows a consumer to control who will receive a copy of his or her credit report, thus making it nearly impossible for criminals to use stolen information to open an account in the consumer's name.[43] Security freeze provisions will become effective in 2 weeks—on July 1, 2005—in two additional states, Louisiana and Vermont.[44]

Although the credit bureaus argue that security freezes are overkill and cause consumers more harm than good, many members of the business community in Vermont supported implementation of our security freeze law enacted last year. Overall, consumer advocates and many State Attorneys General believe that security freeze laws are one of the most effective tools available to stop the harm that can result from data heists. Twenty states considered security freeze bills this past spring.[45] As of today, three of these states enacted the measure: Colorado, Maine, and Washington.[46] The legislatures in Connecticut and Illinois also passed security freeze bills, but these bills have not yet been signed into law.

V. Recommendations on Addressing the Problem of Security Breaches

I recommend that this Committee take several actions to address the security breach problem, with its concomitant potential effect on the increased incidence of identity theft. The recommendations center on enactment of better Federal laws to address the problem, while allowing the states to continue to perform their vital functions in assisting consumers and creating additional innovative solutions.

1. *Enact a Federal Security Breach Notification Law:* Enact a Federal law requiring notice of security breaches in appropriate circumstances. Allow states to enact laws that are more protective of consumers, thus ensuring that states can continue devising additional innovative solutions to this issue.

2. *Enact a Federal Program for Regulation of Data Brokers:* Enact a Federal law to regulate data brokers in a manner similar to regulation of credit reporting agencies. Currently, the regulation of data brokers comes under a scattered mixture of Federal laws, including the Federal Fair Credit Reporting Act, the Gramm-Leach-Bliley Act (GLBA),[47] and a few other laws, and arguably these laws do not cover all the practices of data brokers. In developing a unified Federal regulatory scheme for data brokers, only preempt state laws to the extent that they are less protective of consumers.

3. *Strengthen the "Safeguards Rules":* Enact a Federal law that will strengthen the GLBA Safeguards Rules issued by the Federal financial regulators and the Federal Trade Commission.[48] Currently, these rules require the covered institutions to develop a written information security plan that describes their programs to protect customer information, and to maintain reasonable security for customer information. The rules were intended to provide flexibility to account for each covered institution's size, complexity, scope of activities, and sensitivity of information handled. However, in light of the recent wave of security breaches, we believe that more definitive minimum standards of information security should be required, and that the Safeguards Rules should be expanded to more clearly cover data brokers.

4. *Recognize the Important Role of State Legislative and Investigative Efforts:* States are providing key additional protections for consumers. Security breach notification laws in California, Arkansas, Georgia, Indiana, Montana, North Da-

kota, and Washington State and security freeze laws in California, Louisiana, Texas, Vermont, Colorado, Maine, and Washington State, are important examples of the critical role the states play in developing innovative solutions to the complex problems presented by data breaches. In addition, State Attorneys General and local law enforcement are playing critical roles in the investigations surrounding security breaches that have been disclosed to date. State and local law enforcement officials are cooperating with their Federal counterparts to investigate and prosecute the perpetrators, and to determine if there were defects in security systems that may have allowed the breaches to occur. Congress should recognize these vital functions provided by state and local authorities, and ensure that these functions are not preempted.

Thank you for giving me the opportunity to testify on this important subject.

ENDNOTES

[1] Debaise & Dreazen, *Federal Prosecutors Break Ring of Identity Thieves,* Wall Street Journal, Nov. 26, 2002, available at *http://online.wsj.com/PA@VJBNA4R/article__print/0,,SB1038249179137636588,,00.html*.

[2] UDDOJ, "Milford Man Pleads Guilty to Hacking Intrusion and Theft of Data Cost Company $5.8 Million," Dec. 18, 2003, available at *http://www.usdoj.gov/criminal/cybercrime/baasPlea.htm*.

[3] Sullivan, *Data base Giant Gives Access to Fake Firms; Choicepoint Warns More Than 30,000 They May be at Risk,* MSNBC.com, Feb. 14, 2005, available at *http://www.msnbc.msn.com/id/6969799/print/1/displaymode/1098/; ChoicePoint: More ID theft warnings,* CNN/Money, Feb. 17, 2005, available at *http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/*.

[4] Perez & Brooks, *For Big Vendor of Personal Data, A Theft Lays Bare the Downside,* Wall Street Journal, May 3, 2005, at A1.

[5] Carrns, *Bank of America Missing Tapes with Card Data,* Wall Street Journal, Feb. 28, 2005, at B2.

[6] *Credit Information Stolen From DSW Stores,* AP, Mar. 8, 2005, available at *http://biz.yahoo.com/ap/050308/dsw__credit__cards__4.html?printer=1;* DSW Alerts Customers of Credit Card and Other Purchase Information Security Issues, DSW, Mar. 8, 2005, available at *http://www.dswshoe.com/ccpressrelease/pr/index.html; DWS data theft larger than predicted,* USA Today, Apr. 19, 2005.

[7] El-Rashidi, *LexisNexis Owner Reports Breach of Customer Data,* Wall Street Journal, Mar. 10, 2005, at A3.

[8] "LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access," Apr. 12, 2005, available at *http://www.lexisnexis.com/about/releases/0789.asp.*

[9] Bank & Conkey, *New Safeguards For Your Privacy,* Wall Street Journal, Mar. 24, 2005, at D1.

[10] Fischer & Krupnick, *UC informs people of data security breach,* Contra Costa Times, Apr. 1, 2005, available at *http://www.contracostatimes.com/mld/cctimes/newslocal/states/california/counties/alameda__county/cities__neighborhoods/berkeley/11284658.htm.*

[11] Kawamoto, *Medical Group: Data on 185,000 People was Stolen,* Apr. 8, 2005, available at *http://www.nytimes.com/cnet/CNET__2100–7349__3–5660514.html.*

[12] *Ameritrade loses customer account info,* CNN, Apr. 19, 2005.

[13] Sidel & Conkey, *Security Breach Hits Credit Cards; HSBC Notifies 180,000 People Who Shopped at Ralph Lauren; Other Banks May Be Affected,* Wall Street Journal, Apr. 14, 2005, at D1.

[14] Angwin & Bank, *Time Warner Alerts Staff to Lost Data; Files for 600,000 Workers Vanish During Truck Ride,* Wall Street Journal, May 3, 2005, at A3.

[15] *Bank data Theft Could Hit Nearly 700,000,* AP, May 23, 2005.

[16] *Citi Notifies 3.9 Million Customers of Lost Data,* MSNBC, June 7, 2005, available at *http://www.msnbc.msn.com/id/8119720*.

[17] Cal. Civ. Code §§ 1798.29 and 1798.82.

[18] Cal. Civ. Code § 1798.82(a) and (c); Cal. Civ. Code § 1798.29(a) and (c).

[19] *Id.* at 1798.82(e) and 1798.29(e).

[20] 15 U.S.C.A. § 7001.

[21] Cal. Civ. Code § 1798.82(g) and (h); Cal. Civ. Code § 1798.29(g) and (h).

[22] Sullivan, *Is Your Personal Data Next? Rash of Data Heists Points to Fundamental ID Theft Problem,* MSNBC, Apr. 4, 2005.

[23] Saranow & Leiber, *Freezing Out Identity Theft,* Wall Street Journal, Mar. 15, 2005, at D1.

[24] Synovate, Federal Trade Commission—Identity Theft Survey Report, Sept. 2003, at 9, available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf*. Only about 25 percent of all victims report the crime to local police or to a credit bureau.

The victims of the most serious form of identity theft, involving "new accounts and other frauds," report the crime to law enforcement authorities only 43 percent of the time, and to credit reporting agencies 37 percent of the time. *Id.*

[25] National and State Trends in Fraud & Identity Theft, January–December 2004, FTC, Feb. 1, 2005, at 9, available at *http://www.consumer.gov/idtheft/stats.html*.

[26] *Id.* at 10.

[27] *Id.* at 13.

[28] *Id.* at 14.

[29] Synovate, Federal Trade Commission—Identity Theft Survey Report, Sept. 2003, at 6.

[30] *Id.*

[31] *Id.*

[32] *See, e.g.,* "ChoicePoint to Notify Vermont Consumers Affected by Security Breach," Vermont Attorney General press release, Feb. 24, 2005, available at *http://www.atg.state.vt.us/display.php?pubsec=4&curdoc=881.*

[33] *State of Ohio* v. *DSW, Inc.,* Case No. 05CVH06–6128 (Franklin Cty, OH, June 6, 2005).

[34] Synovate, Federal Trade Commission—Identity Theft Survey Report, Sept. 2003, at 8.

[35] *Id.*

[36] According to the National Conference of State Legislatures, the following states are considering "breach of information" legislation: Alaska, Arizona, Arkansas, Colorado, Georgia, Florida, Illinois, Indiana, Maryland, Michigan, Minnesota, Missouri, Montana, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Washington, and West Virginia. *See* 2005 Breach of Information Legislation, National Conference of State Legislatures, Apr. 1, 2005, available at *http://www.ncsl.org/programs/lis/CIP/priv/breach.htm.* In addition, Massachusetts in also considering a security breach bill. *See, e.g.,* Mass. S.B. 184 (2005).

[37] Ark. Code Ann. §§ 4–110–102 to 108; Fla. Stat. ch. 817.5681; Ga. Code Ann. §§ 10–1–910 to 912; Ind. Code § 4–1–11; Mont. Code Ann. § 31–3–115; N.D. Cent. Code § 51–30–01 to 07; Wash. Rev. Code § 42.17.

[38] Pub. L. No. 108–159 (2003).

[39] *See* 15 U.S.C.A. § 1681t(b)(4), grandfathering in the state provisions allowing free reports in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont.

[40] *See* "Facts for Consumers: Your Access to Free Credit Reports," FTC, available at *http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.*

[41] *See* 15 U.S.C.A. § 1681c–1.

[42] *See* Saranow & Lieber, *Freezing out Identity Theft,* Wall Street Journal, Mar. 15, 2005, at D1.

[43] *See* Cal. Civ. Code § 1785.11.2 (California); V.T.C.A., Bus. & C. § 20.034 (Texas).

[44] *See* LSA–R.S. § 9:3571.1 (Louisiana); 9 V.S.A. § 2480b (Vermont).

[45] According to the National Conference of State Legislatures, the following states are considering security freeze legislation: Colorado, Connecticut, Hawaii, Illinois, Indiana, Kansas, Kentucky, Maine, Maryland, Missouri, Nevada, New Jersey, New Mexico, New York, Oregon, Pennsylvania, South Carolina, Utah, and Washington. *See* Consumer Report Security Freeze Legislation 2005 Session, National Conference of State Legislatures, Mar. 8, 2005, available at *http://www.ncsl.org/programs/banking/SecurityFreeze_2005.htm.* In addition, Massachusetts is considering a security freeze bill. *See, e.g.,* Mass. S.B. 184 (2005).

[46] Colo. Rev. Stat. §§ 12–14.3–106.6 to 106.9 (effective July 1, 2006); Me. Rev. Stat. Ann. tit. 10, §§ 1313–DC to E (effective Feb. 1, 2006); Wash. Rev. Code § 19.182 (effective July 24, 2005).

[47] Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09, and its implementing privacy rule, Privacy of Consumer Financial Information, 16 C.F.R. Part 313.

[48] GLBA requires Federal and state regulators of financial institutions to issue "safeguards rules". *See* 15 U.S.C. § 6801(b). The Federal banking agencies, state insurance authorities, and the Federal Trade Commission all issued comparable safeguards rules. *See, e.g.,* Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8, 616–8, 641 (Feb. 1, 2001). The FTC's Safeguards Rule is found at 16 C.F.R. Part 314.

Senator SMITH. Thank you very, very much for your presence and your testimony, and we will take into consideration, obviously, the things you're requesting. As a former state legislator, many of us, we appreciate that.

Mr. SORRELL. Thank you, Senator.

Senator SMITH. Senator Burns have a——

Senator BURNS. Mr. Chairman?

Senator SMITH.—any of my colleagues have a question?

Senator BURNS. Thank you. I just want to ask a question. Like in Vermont and states, when we talk about people who collate—in other words, your data brokers—that used to be termed, I think, years ago, as their own credit bureaus. They were licensed, they were bonded, they took the information that was given to them by institutions on records, and that could only be accessed by permission of the person, along with the institution desiring the information. Are we headed in that direction, where all data brokers would have to be licensed and bonded and go through that procedure to be a legitimate broker, number one? And, number two, anybody that does that outside of that would be in an illegal business—we're trying to figure out how do we get a handle on this, because by the time you're notified, your information might be passed on to four or five other parties before you can do anything about it. And the biggest damage that we suffer is our credit. Once your credit is destroyed, it takes forever—if it can be restored—it's a very difficult thing.

Mr. SORRELL. I think that there's a balance here. Because if we look at the way the economy functioned in the days of the credit bureaus, that was something that you could fairly readily get a handle on, and it was an important piece, but a relatively small piece of the overall functioning of commerce. Now, in the Information Age, with the ability to collect more information and to transmit more information much more efficiently and effectively, quickly, than was ever the case, I would—and, speaking for myself—want to take a hard look at the negative impacts on the economy if you were to have specific individual registration of everyone that would fit under the umbrella definition of a data broker. Depending on how broad that definition is, you'd need a huge, potentially, regulatory operation to register and enforce. That's why, I think, that creating safeguards that clearly affect and control all those that are in the data-broker—fit under that definition, with minimum standards for any companies that are collecting this personal information that we're talking about today, of what they would need to do, as a minimum, to lock that door to protect that consumer information, makes sense. The specific registration of each individual data broker, I don't, frankly, know, Senator, how many people would fit under that category, and I'm reluctant to——

Senator BURNS. Well——

Mr. SORRELL.—say we should do it.

Senator BURNS. Well, we probably couldn't define, but I finally figured out, though, that the only way, on identity theft—and especially with the credit and credit cards—maybe we should take our credit cards and maintain a balance in our credit cards that would be almost to our limit——

[Laughter.]

Senator BURNS. My wife does a good job of that.

[Laughter.]

Senator BURNS. So that they—no fraud could be committed. In other words, they wouldn't be accepted. But it is the most fearful thing, I think, in my state about people, and—because it has happened—and you just hear horror stories with regard to that.

Mr. SORRELL. One of the things that certain of the states—California, Texas, Louisiana, Vermont, and a couple of other states now have enacted is to use security freeze legislation, which allows the individual consumer to communicate with the credit agencies—that all of the banks look to check your credit, to see whether to extend credit to you—allow you to put a freeze on your credit reports and—so that outside companies cannot access your credit unless you specifically give permission. You're allowed, under state statute, to so-called "thaw" this, so that if you're going for a mortgage or a car loan, that the potential lender will be able to access your record.

Senator SMITH. Senator Nelson had a brief question, as well.

Senator BILL NELSON. Mr. Attorney General, you have described your preference to approach this problem in many of the elements of the legislation that's been filed by several of the Members of this Committee. And you also recommend that the regulation of these data information brokers be similar to the way that we regulate the credit reporting agencies, without all the mumbo-jumbo of the licensing and all of that stuff.

In addition to what you've already said, what—you would certainly embrace the concept of having one-stop shopping, where, identity theft, somebody has a place to go.

Mr. SORRELL. Yes.

Senator BILL NELSON. How about in the overall picture of homeland security, having an Assistant Secretary of Cybersecurity within the Department of Homeland Security?

Mr. SORRELL. Well, I think I understand what you're asking. I think—it sounds like it makes sense to me, Senator.

Senator BILL NELSON. And, clearly, tightening up on the commercial usage of Social Security numbers.

Mr. SORRELL. Yes. I think that that's critical.

Senator BILL NELSON. Do you embrace the concept that we take the model of the California law, notification, and apply that nationally?

Mr. SORRELL. Yes, I do, but with the ability, if states wished, to go further, to be more protective of their citizens, to allow them to do that. Yes, sir.

Senator BILL NELSON. Absolutely, I agree with you that this ought to be a floor upon which the states can build and be more creative.

Mr. SORRELL. Thank you much.

Senator BILL NELSON. How about the concept of utilizing the Federal Trade Commission as the place of the Office of Identity Theft?

Mr. SORRELL. I don't pretend to be fully versed on all the nuances of the different Federal regulatory bodies, but that makes sense to me, from my knowledge.

Senator BILL NELSON. It is the place that governs the credit reporting agencies.

OK, thank you.

Senator SMITH. Thank you, Senator Nelson.

Attorney General Sorrell, thank you for your presence and your testimony today.

Mr. SORRELL. Thank you much.

STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Mr. Chairman, can I say one—

Senator SMITH. Oh.

Senator PRYOR.—very briefly? And that is, I served with General Sorrel when I was the Attorney General in my state—fine person, fine Attorney General, fine public servant. And I think this Committee would really benefit from his thoughts, not just on this, but a number of other subjects, because he has really committed his professional life to try to make his state, and, in some ways, the Nation, better for consumers and for, really, the marketplace. And so, he has been a real leader on this. So, I hope we'll take his words to heart and consider what he has to say.

Senator SMITH. We'll do that, Senator Pryor.

Senator Ben Nelson apparently has a question, too.

STATEMENT OF HON. E. BENJAMIN NELSON, U.S. SENATOR FROM NEBRASKA

Senator BEN NELSON. Thank you, Mr. Chairman.

And, Mr. Attorney General, I have a natural inclination to support states' rights and the right of the state to protect public health, welfare—in this case, the identity of its citizens. There was a point made by Senator Feinstein that there's a real question about preemption here and whether or not there's a conflict where, if we permit every state to do a patchwork quilt of regulation and/or legislation, that it will adversely affect commerce, that it may not facilitate simply identity theft protection, at the risk of harming commerce. And she also said to me—I think it's very optimistic on her part, and I hope it will be—it'll come to pass—and that is that they're trying to work out the whole question of preemption to permit the states to be able to protect at some level, but also recognize the interstate aspects of this.

Could you give us maybe just a little bit more of your opinion about what you think that might consist of——

Mr. SORRELL. Well, I——

Senator BEN NELSON.—and whether it's possible. I certainly hope that it is.

Mr. SORRELL. I think it is possible, Senator. I hear the arguments that we can't have this patchwork quilt of different regulations, but the reality is, as I talked about, as the commerce changes this really is a global economy now. And so, we have many, many different countries that have their own rules and regulations. We certainly, in the environmental arena, have different rules and regulations at the state level, that companies that do business nationally and internationally must abide by when they're doing business in an individual state. And they're—and the beauty of the information that we gather now is that, for many companies, they are looking to market to you, as an individual. They collect information about you, your income level. They collect data from other places about your buying habits. And it's a niche-niche-niche market. And so, the companies that are able to figure out what you, individually, might want, and to market to you, can certainly program their computers to trigger different regulation—give notice of different regulation provisions or standards at a different—certain zip code levels, or whatever.

So, I am not one who buys the argument that we're going to throw a wrench into the works of commerce by allowing states that wish to go forward to do—go further—to do so. And I gave the example of what Vermont has done to better protect our consumers under Gramm-Leach-Bliley legislation that you've enacted.

Senator BEN NELSON. Thank you.

Thank you, Mr. Chairman.

Senator SMITH. Thank you very much.

Senator ALLEN. Mr. Chairman, may I ask——

Senator SMITH. Yes.

Senator ALLEN.—the Attorney General a question?

Senator SMITH. Sure.

STATEMENT OF HON. GEORGE ALLEN, U.S. SENATOR FROM VIRGINIA

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

Attorney General, thank you for being here. And the fact that some states, such as you all, are acting on this shows there's a need for us to strengthen existing laws. In a somewhat analogous situation in dealing with spyware, there are some of us, including the Chairman of the Committee, who recognize this, similar to spyware, is not just in this country, it's national, it's international. There should be a—and the way I'm looking at it is, have a national standard. On spyware, and possibly also on this issue here, of breach of data, or data mining, and so forth, have a national standard, tough standard, give assistance to the FTC to enforce it, but also allow the states attorneys general to also enforce that law. That's another level of enforcement. And could you share with us what your view would be? Let's assume we have a national standard, but allow you and others, attorneys general in the country, to enforce it, with proper enhanced penalties for those who are breaching or committing these sort of frauds. What would your view be of that?

Mr. SORRELL. We, right now, have the ability to protect our consumers against some of these issues with data brokers. For example, through our state consumer-protection laws, unfair and deceptive practices. Giving us—having a Federal standard set, and giving the individual states the ability to enforce that standard, we would welcome that. The reality is, with the numbers, and the burgeoning numbers, of those perpetrating these crimes of identity theft, the numbers of victims—numbers of perpetrators, it will be very difficult for the Federal authorities, alone, to try to catch all the bad guys, and we would welcome the opportunity to have the authority to help in that effort.

Senator ALLEN. Great, thank you. Thank you, Attorney General.

Mr. SORRELL. Thank you.

Senator ALLEN. Thank you, Mr. Chairman.

Senator SMITH. Thank you, Attorney General. We appreciate your presence.

Mr. SORRELL. Thank you much.

Senator SMITH. We will now call to the dais the Federal Trade Commission. We are grateful for their patience. And the first panel—or, this panel will consist of the Honorable Deborah Majoras, Federal Trade Commission Chairman; the Honorable Orson Swindle, Commissioner; the Honorable Thomas B. Leary, Commissioner; the Honorable Pamela Jones Harbour, also a Commissioner; and the Honorable Jon Leibowitz, recently put on the Commission.

I don't know whether my colleagues saw it, but I'll include it in the record, a story in the *Washington Post* this morning, which begins, "Thousands of current and former employees at the Federal Deposit Insurance Corporation are being warned that their sensitive personal information was breached, leading to an unspecified number of fraud cases." That's our challenge—to stop that.

I would also like to note and thank Commissioner Swindle for his service to the FTC. Mr. Swindle is leaving the FTC at the end of the month, and this will be his last time appearing before the Committee. It's well known by many of us that Commissioner Swindle has a distinguished military career, along with his service to protect consumers at the FTC. And, sir, we thank you for your public service.

Commissioner SWINDLE. Thank you, Mr. Chairman.

Senator SMITH. Madam Chairman?

STATEMENT OF HON. DEBORAH PLATT MAJORAS, CHAIRMAN, FEDERAL TRADE COMMISSION

Chairman MAJORAS. Thank you, Mr. Chairman, members of the Committee. I am Deborah Majoras, Chairman of the Federal Trade Commission.

My fellow Commissioners and I appreciate the opportunity to appear before you today as we work to ensure the safety and security of consumers' personal information. The views expressed in the written testimony represent the views of the Commission. Our oral presentations and responses to your questions reflect our own views, and do not necessarily reflect the views of the Commission or any individual Commissioner.

Advances in commerce, computing, and networking have transformed the role of consumer information. New technologies allow businesses to offer consumers a wide range of products and payment options, greater access to credit, and faster transactions. But with these benefits come some concerns about privacy and security of consumer sensitive information and, in particular, the threat of identity theft, which we've heard so much about this morning, and which my colleague, Commissioner Harbour, will address in more detail.

Several current laws protect consumer sensitive information, depending on how that information is collected and how it is used. Both the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, for example, address access to, and the security of, such information in specific contexts.

The Commission has brought five cases against companies, such as Microsoft and Eli Lilly, challenging the failure to maintain adequate data-security procedures. In each of these cases, the Commission alleged that the business misrepresented their privacy or security procedures, in violation of section 5 of the FTC Act.

Today, I am announcing that the Commission has brought and settled its sixth action in this area, this one against BJ's Wholesale Club, a Fortune 500 company with over $6 billion in annual sales. For the first time, we allege that inadequate data security can be an unfair business practice under section 5. This action should provide clear notice to the business community that failure to maintain reasonable and appropriate security measures, in light of the sensitivity of the information, can cause substantial consumer injury and may violate the FTC Act.

Our complaint alleges that BJ's stored personal information from customers' credit and debit cards on computers at its stores, even without a legitimate business reason for doing so, and then failed to take appropriate steps to secure this information. The complaint alleges that, as a result, the customer data that BJ's left unsecured ended up on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. Federal law limits consumers' liability for unauthorized use of the credit or debit card numbers. In this case, after the fraud was discovered, banks canceled and reissued thousands of credit and debit cards, and have turned to BJ's to cover the cost of the identity theft and corrective actions. According to SEC filings, as of May 2005, the amount of outstanding claims was approximately $13 million. Our settlement requires BJ's to establish a comprehensive and rigorous information security program, and to obtain regular security assessments of that program from a qualified independent auditor.

Recent security breaches, such as that alleged in BJ's and all the others we've discussed here this morning, raise questions about whether companies that maintain sensitive personal information are taking adequate steps to protect it.

My colleague to my right, Commissioner Swindle, will discuss the Commission's efforts to promote greater information security.

As detailed in our written testimony, as this Committee is considering whether to enact new procedures for sensitive consumer data—protections for sensitive consumer data, several measures should be considered.

First, Congress should consider whether companies that maintain sensitive consumer information should be required to implement reasonable security procedures. Any such requirement could be patterned after the Commission's Safeguards Rule under GLB. The Safeguards Rule provides a strong, but flexible, requirement to make sure that information is maintained securely. It recognizes that security is an ongoing process, and not a set of technical standards. Currently, the Safeguards Rule applies only to customer information collected by financial institutions. I believe the same principles embodied in that rule makes sense for other entities that maintain sensitive information.

Second, Congress should consider whether to require firms to notify consumers if sensitive information about them has been breached in a way that creates a significant risk of identity theft.

Obviously, many people agree that prompt notice in appropriate circumstances can help consumers avoid or mitigate identity theft. At the same time, however, requiring notices for security breaches that pose little or no risk may create confusion, even panic, and impose unnecessary costs. For example, consumers may cancel credit cards or place fraud alerts on their credit files even if such measures are not needed and, not to mention, may suffer from unwarranted worry and stress. Perhaps more importantly, if notices are sent too often, consumers will become numb to them and will fail to pay attention.

Formulating the right balance is difficult, and there are different notices that could be considered. One, of course, is, in effect, promulgated by the Federal banking agencies, and another is in effect in California. And we think both of those deserve a close look.

If Congress decides to enact a national breach requirement, it might consider authorizing the FTC to conduct a rulemaking to specify a standard that best meets the needs of consumers. Through a rulemaking, we could examine the different standards that have already been operating and determine how well they have worked.

A third area for consideration is possible restrictions on the selling of Social Security numbers. My colleague, Commissioner Leary, will address Social Security numbers in greater detail.

And, finally, given the globalization of the marketplace, effective law enforcement against security breaches will require effective cross-border efforts. Accordingly, the Commission recommends that Congress enact cross-border fraud legislation, which my colleague, Commissioner Leibowitz, will discuss in more detail.

Mr. Chairman and Members of the Commission, thank you for your attention and for the opportunity to be here. And I welcome any questions you may have.

[The prepared statement of Chairman Majoras follows:]

PREPARED STATEMENT OF HON. DEBORAH PLATT MAJORAS, CHAIRMAN, FEDERAL TRADE COMMISSION

I. Introduction

Mr. Chairman, I am Deborah Platt Majoras, Chairman of the Federal Trade Commission.[1] My fellow Commissioners and I appreciate the opportunity to appear before you today as we work to ensure the safety and security of consumers' personal information.

As we have testified previously, advances in commerce, computing, and networking have transformed the role of consumer information. Modern consumer information systems can collect, assemble, and analyze information from disparate sources, and transmit it almost instantaneously. Among other things, this technology allows businesses to offer consumers a wider range of products, services, and payment options; greater access to credit; and faster transactions.

Efficient information systems—data that can be easily accessed, compiled, and transferred—also can lead to concerns about privacy and security. Recent events validate concerns about information systems' vulnerabilities to misuse, including identity theft.

II. Background

One particular focus of concern has been "data brokers," companies that specialize in the collection and distribution of consumer data. Data brokers epitomize the tension between the benefits of information flow and the risks of identity theft and other harms. Data brokers have emerged to meet the information needs of a broad spectrum of commercial and government users.[2] The data broker industry is large and complex and includes companies of all sizes. Some collect information from original sources, both public and private; others resell data collected by others; and many do both. Some provide information only to government agencies or large companies, while others sell information to smaller companies or the general public as well. The amount and scope of the information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. These uses include fraud prevention, debt collection, law enforcement, legal compliance, applicant authentication, market research, and almost any other function that requires the collection and aggregation of consumer data. Because these databases compile sensitive information, they are especially attractive targets for identity thieves.

Identity theft is a crime that harms both consumers and businesses. A 2003 FTC survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses.[3] The survey looked at the two major categories of identity theft: (1) the misuse of existing accounts; and (2) the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, in both the time and money spent resolving the problems. For example, although people who had new accounts opened in their names made up only one-third of the victims, they suffered two-thirds of the direct financial harm. The ID theft survey also found that victims of the two major categories of identity theft cumulatively spent almost 300 million hours—or an average of 30 hours per person—correcting their records and reclaiming their good names. Identity theft causes significant economic and emotional injury, and we take seriously the need to reduce it.

As detailed in our recent testimony on this subject,[4] there are a variety of existing Federal laws and regulations that address the security of, and access to, sensitive information that these companies maintain, depending on how that information was collected and how it is used. For example, the Fair Credit Reporting Act (FCRA)[5] regulates credit bureaus, any entity or individual who uses credit reports, and the businesses that furnish information to credit bureaus.[6] The FCRA requires that sensitive credit report information be used only for certain permitted purposes. The Gramm-Leach-Bliley Act (GLBA)[7] prohibits financial institutions from disclosing consumer information to non-affiliated third parties without first allowing consumers to opt out of the disclosure. GLBA also requires these businesses to implement appropriate safeguards to protect the security and integrity of their customer information.[8]

In addition, Section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce."[9] Under the FTC Act, the Commission has broad jurisdiction to prohibit unfair or deceptive practices by a wide variety of entities and individuals operating in commerce. Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.[10] To date, the Commission has brought five cases against companies for deceptive security claims.[11] These actions alleged that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information, but because they allegedly failed to take such steps, their claims were deceptive. The consent orders settling these cases have required the companies to implement appropriate information security programs that generally conform to the standards that the Commission set forth in the GLBA Safeguards Rule.

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.[12] The Commission has used this authority to challenge a variety of injurious practices that threaten data security.[13]

As the Commission has testified previously, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate.[14] It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution.[15]

Despite the existence of these laws, recent security breaches have raised questions about whether data brokers and other companies that collect or maintain sensitive personal information are taking adequate steps to ensure that the information they possess does not fall into the wrong hands, as well as about what steps should be taken when such data is acquired by unauthorized individuals. Vigorous enforcement of existing laws and business education about the requirements of existing laws and the importance of good security can go a long way in addressing these concerns. Nonetheless, recent data breaches have prompted Congress to consider legislative proposals, and the Commission has been asked to comment on the need for new legal requirements.

III. Increasing Consumer Information Security

The Commission recommends that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions.

Further, the Commission recommends that Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft.[16] Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. As discussed below, the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required.

In addition, many have raised concerns about misuse of Social Security numbers. It is critical to remember that Social Security numbers are vital to current information flows in the granting and use of credit and the provision of financial services. In addition, private and public entities routinely have used Social Security numbers for many years to access their voluminous records. Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers.

Finally, law enforcement activity to protect data security is increasingly international in nature. Given the globalization of the marketplace, an increasing amount of U.S. consumer information may be accessed illegally by third parties outside the United States or located in offshore databases. Accordingly, the Commission needs new tools to investigate whether companies are complying with U.S. legal requirements to maintain the security of this information, and cross-border fraud legislation would give the Commission these tools. For that reason, the Commission recommends that Congress enact cross-border fraud legislation to overcome existing obstacles to information sharing and information gathering in cross-border investigations and law enforcement actions.[17]

For example, if the FTC and a foreign consumer protection agency are investigating a foreign business for conduct that violates both U.S. law and the foreign country's law, current law does not authorize the Commission to share investigative information with the foreign consumer protection agency, even if such sharing would further our own investigation. New cross-border fraud legislation could ease these restrictions, permit the sharing of appropriate investigative information with our foreign counterparts, and give us additional mechanisms to help protect the security of U.S. consumers' data whether it is located abroad or in the United States.

A. Require Procedures To Safeguard Sensitive Information

One important step to reduce the threat of identity theft is to increase the security of certain types of sensitive consumer information that could be used by identity thieves to misuse existing accounts or to open new accounts, such as Social Security numbers, driver's license numbers, and account numbers in combination with required access codes or passwords.[18] Currently, the Commission's Safeguards Rule under GLBA requires financial institutions to implement reasonable physical, technical, and procedural safeguards to protect customer information. Instead of mandating specific technical requirements that may not be appropriate for all entities and might quickly become obsolete, the Safeguards Rule requires companies to evaluate the nature and risks of their particular information systems and the sensitivity of the information they maintain, and to take appropriate steps to counter these threats. They also must periodically review their data security policies and procedures and update them as necessary. The Safeguards Rule provides a strong but flexible framework for companies to take responsibility for the security of information in their possession, and it reflects widely accepted principles of information security, similar to those contained in the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems and Networks.[19]

Currently, the Safeguards Rule applies only to "customer information" collected by "financial institutions."[20] It does not cover many other entities that may also collect, maintain and transfer or sell sensitive consumer information. Although we believe that Section 5 already requires companies holding sensitive data to have in place procedures to secure it if the failure to do so is likely to cause substantial consumer injury, we believe Congress should consider whether new legislation incorporating the flexible standard of the Commission's Safeguards Rule is appropriate.

B. Notice When Sensitive Information Has Been Breached

Unfortunately, even if the best efforts to safeguard data are made, security breaches can still occur. The Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified. Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft. Notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves.

The challenge is to require notices only when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally.

Currently there are two basic approaches in place that are used to determine when notices should be triggered. The first is the bank regulatory agency standard.[21] Under that standard, notice to the Federal regulatory agency is required as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, notice to consumers is required when, based on a reasonable investigation of an incident of unauthorized access to sensitive customer information, the financial institution determines that misuse of its information about a customer has occurred or is reasonably possible.[22]

The second approach is found in the California notice statute.[23] Under that approach, all businesses are required to provide notices to their consumers when a defined set of sensitive data, in combination with information that can be used to identify the consumer, has been or is reasonably likely to have been acquired by an unauthorized person in a manner that "compromises the security, confidentiality, or integrity of personal information."[24]

The California "unauthorized acquisition" approach to requiring consumer notice does not compel notice in every instance of improper access to a database. Instead, it allows businesses some flexibility to determine when a notice is necessary, while also providing a fairly objective standard against which compliance can be measured by the broad range of businesses subject to the law. Under guidance issued by the California Office of Privacy Protection, a variety of factors can be considered in determining whether information has been "acquired," such as: (1) indications that protected data is in the physical possession and control of an unauthorized person (such as a lost or stolen computer or other device); (2) indications that protected data has been downloaded or copied; or (3) indications that protected data has been used by an unauthorized person, such as to open new accounts.[25] One issue that is not directly considered is what action to take in cases in which, prior to sending consumer notification, the business already has taken steps that remedy the risk. For example, one factor to consider in deciding whether to provide notice is whether the business already has canceled consumers' credit card accounts and reissued account numbers to the affected consumers.

We have growing experience under both models to inform consideration of an appropriate national standard. Because formulating any standard will require balancing the need for a clear, enforceable standard with ensuring, to the extent possible, that notices go to consumers only where there is a risk of harm, we believe that if Congress decides to enact a notice provision, the best approach would be to authorize the FTC to conduct a rulemaking under general statutory standards. The rulemaking would set the criteria under which notice would be required for data breaches involving non-regulated industries. The rulemaking could address issues such as the circumstances under which notice is required, which could depend on the type of breach and risk of harm, and the appropriate form of notice. This approach would also allow the Commission to adjust the standard as it gains experience with its implementation.

C. Social Security Numbers

Social Security numbers today are a vital instrument of interstate commerce. With 300 million American consumers, many of whom share the same name,[26] the unique 9-digit Social Security number is a key identification tool for business. As the Commission found in last year's data matching study under FACTA, Social Security numbers also are one of the primary tools that credit bureaus use to ensure that the data furnished to them is placed in the right file and that they are providing a credit report on the right consumer.[27] Social Security numbers are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. Social Security number databases are used to fight identity fraud—for example, they can confirm that a Social Security number belongs to a particular loan applicant and is not stolen.[28] Without the ability to use Social Security numbers as personal identifiers and fraud prevention tools, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

While Social Security numbers have important legitimate uses, their unauthorized use can facilitate identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Currently, there are various Federal laws that place some restrictions on the disclosure of specific types of information under certain circumstances. The FCRA, for example, limits the provision of "consumer report" information to certain purposes, primarily those determining consumers' eligibility for certain transactions, such as extending credit, employment, or insurance. GLBA requires that "financial institutions"[29] provide consumers an opportunity to opt out before disclosing their personal information to third parties, outside of specific exceptions, such as for fraud prevention or legal compliance.[30] Other statutes that limit information disclosure include the privacy rule under the Health Insurance Portability and Accountability Act of 1996,[31] which applies to health care providers and other medical-related entities, and the Drivers Privacy Protection Act,[32] which protects consumers from improper disclosures of driver's license information by state motor vehicle departments.

While these laws provide important privacy protections within their respective sectors, they do not provide comprehensive protection for Social Security numbers.[33] For example, disclosure of a consumer's name, address, and Social Security number may be restricted under GLBA when the source of the information is a financial institution,[34] but in many cases the same information can be purchased on the Internet from a non-financial institution. The problem of how to strengthen or expand existing protections in ways that would not interfere with the beneficial uses of Social Security numbers is challenging.

Although the Commission has extensive experience with identity theft and the consumer credit reporting system, restrictions on disclosure of Social Security numbers could have a broad impact on areas where the Commission does not have expertise. These areas include public health, criminal law enforcement, and anti-terrorism efforts. Moreover, efforts to restrict disclosure of Social Security numbers are complicated by the fact that among the primary sources of Social Security numbers are the public records on file with many courts and clerks in cities and counties across the Nation. Regulation or restriction of Social Security numbers in public records thus poses substantial policy and practical concerns.

Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers. The Commission would appreciate the opportunity to work with Congress to further evaluate the costs and benefits to consumers and the economy of regulating the collection, transfer, and use of Social Security numbers.

IV. Conclusion

New information systems have brought benefits to consumers and businesses alike. Never before has information been so portable, accessible, and flexible. Indeed, sensitive personal financial information has become the new currency of today's high tech payment systems. But with these advances come new risks, and identity thieves and other bad actors have begun to take advantage of new technologies for their own purposes. As the recent focus on information security has demonstrated, Americans take their privacy seriously, and we must ensure that the many benefits of the modern information age are not diminished by these threats to consumers' security. The Commission is committed to ensuring the continued security of consumers' personal information and looks forward to working with you to protect consumers.

ENDNOTES

[1] This written statement reflects the views of the Federal Trade Commission. Our oral statements and responses to any questions you may have represent the views of individual Commissioners and do not necessarily reflect the views of the Commission.

[2] For more information on how consumer data is collected, distributed, and used, see generally Government Accountability Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this Information* (GAO–04–11) (2004); Government Accountability Office, *Social Security Numbers: Use is Widespread and Protections Vary, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO–04–768T) (statement of Barbara D. Bovbjerg, June 15, 2004); Federal Trade Commission, *Individual Reference Services: A Report to Congress* (December 1997), available at *http://www.ftc.gov/os/1997/12/irs.pdf*). The Commission also has held two workshops on the collection and use of consumer information: "Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information," was held on June 18, 2003; and "The Information Marketplace: Merging and Exchanging Consumer Data," was held on March 13, 2001. An agenda, participant biographies, and a transcript for these workshops are available at *http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html* and *http://www.ftc.gov/bcp/workshops/infomktplace/index.html*, respectively.

[3] Federal Trade Commission, *Identity Theft Survey Report* (Sept. 2003), *available at http://www.ftc.gov/os/2003/09/synovatereport.pdf*.

[4] *See, e.g.,* Statement of the Federal Trade Commission Before the Subcommittee on Financial Institutions and Consumer Credit, Committee on Financial Services, U.S. House of Representatives, on Enhancing Data Security: The Regulators' Perspective (May 18, 2005), *available at http://www.ftc.gov/opa/2005/05/databrokertest.htm*.

[5] 15 U.S.C. §§ 1681–1681x.

[6] Credit bureaus are also known as "consumer reporting agencies."

[7] 15 U.S.C. §§ 6801–09.

[8] The FTC's Safeguards Rule implements GLBA's security requirements for entities under the FTC's jurisdiction. *See* 16 C.F.R. pt. 314 ("GLBA Safeguards Rule"). The Federal banking regulators also have issued comparable regulations for the entities under their jurisdiction.

[9] 15 U.S.C. § 45(a).

[10] Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.,* 103 FTC 110 (1984).

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

[12] 15 U.S.C. § 45(n).

[13] These include, for example, unauthorized charges in connection with "phishing," which are high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. *See FTC* v. *Hill*, Civ. No. H 03–5537 (filed S.D. Tex. Dec. 3, 2003), available at *http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm*; *FTC* v. *C.J.*, Civ. No. 03–CV–5275–GHK (RZX) (filed C.D. Cal. July 24, 2003), available at *http://www.ftc.gov/os/2003/07/phishingcomp.pdf*.

[14] *See* Statement of the Federal Trade Commission Before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform (Apr. 21, 2004) at 5, available at *http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf*.

[15] *Id.* at 4.

[16] Commissioner Harbour is concerned about the use of the term "significant" to characterize the level of risk of identity theft that should trigger a notice to consumers.

[17] The U.S. Senate passed cross-border fraud legislation last year by unanimous consent: S. 1234 ("International Consumer Protection Act").

[18] The FTC also would seek civil penalty authority for its enforcement of these provisions. A civil penalty is often the most appropriate remedy in cases where consumer redress is impracticable and where it is difficult to compute an ill-gotten gain that should be disgorged from a defendant.

[19] FTC Commissioner Orson Swindle led the U.S. delegation to the OECD Committee that drafted the 2002 OECD Security Guidelines. *See* Organization for Economic Cooperation and Development, *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security* (July 25, 2002), available at *http://www.oecd.org/document/42/0,2340,en__2649__34255__15582250__1__1__1__1,00.html*.

[20] Under GLBA, a "financial institution" is defined as an entity that engages in one or more of the specific activities listed in the Bank Holding Company Act and its implementing regulations. *See* 15 U.S.C. § 6809(3). These activities include extending credit, brokering loans, financial advising, and credit reporting.

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

[22] Under the guidance, this determination can be made by the financial institution in consultation with its primary Federal regulator.

[23] Cal. Civ. Code § 1798.82.

[24] *Id.* at § 1798.82(d).

[25] These factors are discussed in the California Office of Privacy Protection's publication, *Recommended Practices on Notification of Security Breach Involving Personal Information*, at 11 (Oct. 10, 2003), available at *http://www.privacy.ca.gov/recommendations/secbreach.pdf.*

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

[27] *See* Federal Trade Commission, *Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38–40 (Dec. 2004), available at *http://www.ftc.gov/reports/facta/041209factarpt.pdf*.

[28] The Federal Government also uses Social Security numbers as an identifier. For example, HHS uses it as the Medicare identification number, and the IRS uses it as the Taxpayer Identification Number. It also is used to administer the Federal jury system, Federal welfare and workmen's compensation programs, and the military draft registration. *See* Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), available at *www.ssa.gov/history/reports/ssnreportc2.html.*

[29] *See supra* n.20 (defining financial institution).

[30] GLBA protects some, but not all Social Security numbers held by financial institutions. It does not, for example, cover Social Security numbers in databases of Social Security numbers furnished by banks to credit bureaus under the Fair Credit Reporting Act (*i.e.,* so-called "credit header" information) prior to the GLBA Privacy Rule's July 2001 effective date.

[31] 45 C.F.R. pts. 160 and 164 (implementing Sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191).

[32] 18 U.S.C. §§ 2721–25.

[33] The Commission may, however, bring enforcement actions under Section 5 of the Federal Trade Commission Act against entities whose privacy or security practices are unfair or deceptive.

[34] *See supra* n.30 (discussing limitations of GLBA protection).

Senator SMITH. Thank you, Chairman Majoras.

I think we'll go to Commissioner Swindle.

STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION

Commissioner SWINDLE. Thank you, Mr. Chairman and members of the Committee. And I also thank you very much for your comments and the courtesies that have been shown to me by this Committee, its Members, and its staff. It has really been a pleasure working with you, as well as with the Federal Trade Commission.

Information security is a complex and huge issue involving many challenges, such as database intrusions, theft of sensitive information, viruses, and phishing. And recent headlines in the news have certainly brought into dramatic focus the need for data security. The FTC has been actively involved in promoting the importance of information security. And, personally, information security has been a passion of mine for several years.

The FTC has held workshops with representatives from industry, from Congress, consumer groups, government agencies, and international organizations in an effort to educate ourselves, as well as others, about the issues, and to explore possible solutions to securing electronic data. We also have taken law enforcement action against companies failing to keep promises that they would keep consumers' personal information secure. In addition, the FTC has focused on educating businesses and consumers about the importance of information security.

Security begins with people, each individual being aware of the risk and the importance of doing their part to keep information secure. We simply must establish a culture of security in this country, and—as was mentioned earlier, this is a global economy—and, therefore, the world, where security awareness and the best practices become a subconscious, yet reliable, aspect of our daily lives.

Despite recent security-breach revelations, it is important to recognize that many businesses are making progress and improving information security. On the other hand, it's quite obvious many businesses do not appear to have raised the issue of information security to the CEO/Board-of-Directors level. CEOs must make information-security and privacy-protection practices a priority, devoting the necessary resources to the issue.

Information security and privacy must become part of the corporate or organizational culture. In today's world, information is currency. Businesses take great steps to protect their money. They need to treat information the same way. It is their responsibility, at the highest levels of authority.

New or refined laws may be necessary. New technologies certainly will help. But we must remember that poorly thought-out legislation can have unintended and, often, adverse consequences. Neither new laws, nor new technologies, will provide perfect solutions. Consumers and businesses must properly use the available technical tools and employ responsible information security practices. This, alone, could significantly reduce breaches.

Information security is a complex problem. We all must recognize that achieving good information security is a journey, not a destination. This will be a challenge for all of us for many years to come.

And, in the immediate future, I look forward to answering your questions. Thank you very much, again.

Senator SMITH. Thank you, Commissioner Swindle.

Mr. Leary?

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

Commissioner LEARY. Thank you, Mr. Chairman and Members of the Committee.

I'm pleased to testify here today with my fellow Commissioners on these important issues. I endorse the collective views expressed in the Commission's written testimony, and will, here, add some individual views on Social Security numbers.

As explained in our written testimony, Social Security numbers have many important legitimate uses. Instant access to credit, which we all rely on for both large and small transactions, would be compromised if Social Security numbers could not be used to match consumers to their financial information. Social-Security-number databases are also used for other worthwhile purposes. For example, to locate lost beneficiaries, potential witnesses and law violators, and to collect child support and other judgments.

At the same time, we all recognize that Social Security numbers are sensitive. There is no question that identity thieves can use Social Security numbers as a key to access other people's financial resources. The challenge is to find the proper balance between the need to keep Social Security numbers out of the hands of identity thieves and the ability of businesses to have sufficient information to spot fraud and attribute information to the correct person.

The Federal Trade Commission, as you know, has done considerable research on the overall scope of the identity theft problem. In all candor, however, I personally do not think that we will ever be able to estimate with precision the extent to which misuse of Social Security numbers contributes to this problem or the downside costs of any particular effort to revamp the way Social Security numbers are handled. Congress, itself, will have to make some tough policy decisions.

I also personally believe that the most promising approach would be to consider an extension of the Gramm-Leach-Bliley Act's safeguards rule beyond financial institutions and focus on the way sensitive information is handled, rather than to pass laws that would prohibit myriad private agencies from collecting and preserving sensitive information in the first place. You still have to recognize that a principal source of Social Security numbers today is public records on file with every court and country clerk across the Nation. Restriction of access to this information would raise particularly difficult issues.

We should, however, consider ways to discourage the routine collection of Social Security numbers in circumstances where it is not essential to have such a unique identifier. This might be a very difficult matter to legislate, but, at the very least, we might start with the more active encouragement of private business initiatives and prudent actions by consumers, themselves.

Thank you very much.

Senator SMITH. Thank you, Commissioner Leary.

Commissioner Harbour?

STATEMENT OF HON. PAMELA JONES HARBOUR, COMMISSIONER, FEDERAL TRADE COMMISSION

Commissioner HARBOUR. Mr. Chairman, Senators, I am pleased to address a topic of great importance to the American people, the privacy and security of their most proprietary information.

Almost weekly, it seems, a new story emerges about a company or institution where files containing sensitive information have been compromised, lost, or stolen. These data breaches have been particularly frightening for consumers who fear identity theft. Their apprehension is justified. Our 2003 survey showed that ten million victims had experienced some form of identity fraud in

2002, with an out-of-pocket cost of roughly $5 billion. Our survey also showed that victims of identity theft believed they would have been helped by greater consumer awareness and vigilance about how to safeguard their personal information. Victims also wanted more responsive local law enforcers and stiffer penalties for offenders.

Under Congressional mandate, the Commission has established an extensive program to educate consumers and law enforcers about identity theft, and to assist identity-theft victims.

Consumers may face the greatest risk from security breaches or poor practices by data brokers, because information kept by brokers can be easily used to create new accounts. Accordingly, I believe that data brokers should not be allowed to buy, sell, or transfer Social Security numbers, driver's licenses, and other sensitive personally identifiable information, except for specific permissible purposes, such as law enforcement, anti-fraud measures, and certain legal requirements.

As consumers gain awareness that their personal information is being bought and sold by data brokers, it might be useful to consider whether the fair information practice principles of notice, consent, access, security, and enforcement, could be considered or used to elucidate this area. It is also worth considering that inaccurate data, as well as data that is stolen or misused, can have serious consequences for consumers. Perhaps those who use such data can improve its accuracy by way of best practices.

Finally, nationwide notification to potential victims in the event of a security breach is a necessity. Notification is not just good business guidance; it should be the law whenever there is a risk of harm to consumers due to a security breach. If consumers know as soon as possible that it is reasonably likely their sensitive information has been compromised, they can take steps immediately to mitigate any possible damage, such as monitoring their accounts or availing themselves of the benefits FACTA provides.

And, in conclusion, our national economy increasingly depends on transactions that require the provision of sensitive data. Our challenge in this electronic era is to strike the right balance between the right to information and the right to privacy. To protect sensitive data, we must develop strong policies that nurture and enable the Information Age by encouraging good use of technology while also raising consumer awareness. I'm pleased to work with Members of Congress to address this solution.

Thank you.

Senator SMITH. Thank you very much, Commissioner Harbour.

Commissioner Leibowitz?

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

Commissioner LEIBOWITZ. Good morning, Mr. Chairman and members of the Committee. It's always great to be back here, especially when it's not my nomination hearing.

We were all stunned to learn about Citigroup's computer tapes that were lost during UPS transit. Senator Nelson, you mentioned that earlier. Senator Feinstein did, too. But what struck me the most was a remark by one privacy advocate in a *New York Times* story on the breach. She said, and I'll just read it to you, "Your every day dumpster diver may not know what to do with these tapes, but if these tapes ever find their way into the hands of an international crime ring, I think they'll figure it out."

Let's hope by now these tapes are either buried deeply in a landfill or that they're soon recovered untouched, but the truth is that consumers' personal information is being compromised every day, and that the data-security problem is not confined to U.S. borders. Indeed, American consumers routinely divulge personal information to foreign websites, they routinely share credit-card numbers with telemarketers from around the world, and they routinely receive spam from the distant corners of the globe.

Let me share just a few disturbing examples with you. A foreign website selling to U.S. consumers states that, "We take all reasonable steps to safeguard your personal information." In fact, they don't. The company posts sensitive consumer data in a publicly accessible manner.

Or, thieves from Eastern Europe use spyware to track U.S. consumers' keystrokes as they shop over the Internet.

Or, overseas telemarketers obtain U.S. consumers' bank-account information under false pretenses—we call that pretexting—and use it to wipe out their accounts.

Sadly, these scenarios are based on real investigations, many of which, unfortunately, are difficult for us to pursue, because of limits on our ability to exchange information with foreign law enforcement partners.

Mr. Chairman, the Commission expects to issue a report later this summer that details the harm caused by transnational fraud and the serious challenges we face in investigating these international cases. Foreign law enforcement agencies may be unwilling to share information with the FTC, because we cannot sufficiently guarantee the confidentiality of that information. And we are prohibited from sharing certain information we obtain in investigations with our foreign counterparts, even if sharing information would result in helping to stop fraud against U.S. consumers.

To be sure, there is no panacea for the problems of international data-security breaches, but legislation allowing us to exchange information with foreign law enforcers under appropriate circumstances would be a step forward.

The bottom line is this: If you want the FTC to be more effective in stopping spam, spyware, and security breaches, you need to give us the tools to pursue data crooks across borders.

Mr. Chairman, I won't go into detail about the legislation. I know that you're looking at a draft of the bill, for which we are enormously grateful. The draft is almost identical to the noncontroversial measure Senators McCain and Hollings moved unanimously through your Committee in the Senate in the previous Congress. It still includes those minor changes made last year to address the concerns of industry and privacy groups.

Again, though, thank you for your willingness to listen to us today. Along with my colleagues, I'd be happy to take any questions.

Senator SMITH. Thank you all so very much.

In the interest of order, we'll have questionings in the order arrived. And I have that list in front of me. After my questions, Senator Bill Nelson, Senator Burns, and Senator Ben Nelson. If our other colleagues come back, we will insert them in as they had arrived.

To all of you, in your testimony you stated that companies should be required to notify consumers of a breach when the breach, "creates a significant risk of identity theft." How would the Commission define "significant risk?"

Chairman MAJORAS. Thank you, Mr. Chairman.

You raise the toughest point on this issue. We have been criticized at times, in fact, by those who think significant risk it not the right standard. The key here is completely definitional. What we need to do is, we need to look at instances in which we most certainly would want to have notice given to consumers, and instances in which we haven't.

If you look, for example, at what the State of California has done, the standard looks broad, but then if you look at what the Office of Privacy in California has done, it accepts a long list of types of breaches that, in general, do not present risks of identity theft.

So, what we would do, for example, in a rulemaking, or, obviously, in working with the Committee on a piece of legislation, is try to define those instances in which we believe consumers would most be at risk, or perhaps even except those where they would not be so—for example, if data were encrypted.

Senator SMITH. And would that definition, whatever we ultimately arrive at its meaning, would that then trigger notification to the consumer?

Chairman MAJORAS. Yes, it would.

Senator SMITH. Some forms of security-related breaches may not pose a threat to having one's identity stolen, but might be defined as such. We need to find a sensible solution to determining when individuals should be notified that their personal information may be at risk. What do you all believe is the appropriate standard for determining whether to notify consumers that their identity has, or may have, been stolen?

Chairman MAJORAS. Well, it really just goes back to what I was——

Senator SMITH. Back to the list.

Chairman MAJORAS. I'm sorry. I think you would have to go back to the list. And one of the advantages, Senator, in doing it in a rulemaking context, as opposed to trying to do all specific instances in the statute, is that then we have the freedom to change it as we perceive changes in the marketplace and new threats to consumers.

Senator SMITH. To the issue of preemption of states—you've heard that talked a lot about—should it be a floor or a ceiling? Should we preempt the states? Should we have a national standard?

Chairman MAJORAS. Well, I think—are you asking specifically about notice?

Senator SMITH. Yes.

Chairman MAJORAS. Because there could be other parts of the bill where preemption—where we might answer the question differently.

This is a difficult question. No one ever likes to have to preempt the states. What I would offer to you is that, if you provide a Federal standard that is defined as a floor, as opposed to a ceiling, I'm not sure why you would spend time imposing it at all, because I do think that businesses are going to have to respond to the very highest standard. They can't—I don't think they can chop up their customer lists into 50 different standards, for example. And so, that's just a reality, and it's something to think about, if you want to have a Federal standard at all.

Senator SMITH. To the issue of Social Security numbers, you know Senator Burns and I were talking about how broadly we use them. They were created for one purpose; and that was your Social Security account. But now I understand they're even using them on dog tags in the military. We give them out whenever we're asked to—in various circumstances.

In your opinion, where do you think the use in sharing of Social Security numbers ought to be accessible, or should we begin trying to limit their use for other—for non-Social-Security purposes?

Commissioner LEARY. Well, Senator, I'll jump in on that one. I certainly agree with you, 100 percent, that Social Security numbers evolved very quickly away from their original purpose.

I'll just give you a personal example. When I got my first Social Security number, almost 60 years ago, we were instructed to carry our Social Security card around with us at all times. If you lost your wallet, you would lose your Social Security card. The Internal Revenue Service asked us to put our Social Security number on the envelope when we were mailing in a check, in order to facilitate their filing of it.

So, for people my age, the ship has sailed, as a practical matter. I am certain that my Social Security number is out there in so many places that anyone could find it in 3 minutes.

You have however, a new generation coming in, and you also have I think, a very interesting interim period before we may be able to have even more rigorous individual identifiers, which will enable people to figure out who you are a lot more accurately even than the Social Security number will.

So, the question is, what is worth doing during this interim period of time? And it is a very, very difficult issue. One of the things I wanted to make clear to you, is that this is not arithmetic, where you can figure out what the costs and benefits are of doing it. You're going to have to make these tough value judgments.

I am encouraged by the fact that there is a growing awareness of the problem that you've addressed, and that we now have options. For example, you can now get a driver's license—or you certainly can in the District of Columbia and, I expect, in most states—that no longer have your Social Security number on them. That's a useful first step. We are cautioned not to give away Social Security numbers to people who have no legitimate reasons for them. I would hope that universities would not cease the routine use of Social Security numbers to identify their students who are making purchases in their stores.

All of these things, I think, show a growing awareness of this issue. But to try to put the cork in the bottle retroactively, I suggest to you, is a very difficult thing to do legislatively.

Senator SMITH. My time on that first round is up.

Senator Bill Nelson?

Senator BILL NELSON. Thank you, Mr. Chairman.

I want to thank each of you for your public service. And, Mr. Swindle, thank you for your exceptional service to our country. And godspeed on your—the next chapter of your life.

Commissioner SWINDLE. Thank you.

Senator BILL NELSON. I want to ask each of you to respond to a series of goals which I think is in legislation that is before this Committee. And I think it will help the Committee as we develop a composite piece of legislation. And I'll go right down the line in the order in which you have used—first with Madam Chairman. And if you all could keep your answers short so that I can get all of this information—please respond whether you support the following goals.

Requiring all businesses to take reasonable steps to safeguard sensitive personal information.

Chairman MAJORAS. Yes.

Senator BILL NELSON. Mr. Swindle?

Commissioner SWINDLE. Yes.

Senator BILL NELSON. Mr. Leary?

Commissioner LEARY. Yes.

Senator BILL NELSON. Ms. Harbour?

Commissioner HARBOUR. Yes.

Senator BILL NELSON. Mr. Leibowitz?

Commissioner LEIBOWITZ. Yes.

Senator BILL NELSON. OK.

The next goal. Requiring all businesses to notify customers when their sensitive personal information was, or reasonably believed to have been, acquired by an unauthorized person?

Madam Chairman?

Chairman MAJORAS. It depends on the risk to consumers, for identity theft. If there's a significant risk, then yes.

Commissioner SWINDLE. I agree with the Chairman.

Commissioner LEARY. I agree with the Chairman.

Commissioner HARBOUR. I believe that if there is a risk present, yes, then they should be notified. And, again, I do agree with the Chairman, that it is a definitional question.

Senator BILL NELSON. Mr. Leibowitz?

Commissioner LEIBOWITZ. I agree with notification if there is significant risk or material risk—there needs to be some sort of trigger.

Senator BILL NELSON. Thank you.

Next goal. Requiring that all data brokers register with the FTC so that consumers can find out who has their sensitive information.

Chairman MAJORAS. No, not as stated.

Commissioner SWINDLE. I don't think we can answer that question, because it involves establishing a new regulatory regime for something that we don't really know the details on.

Commissioner LEARY. No.

Commissioner HARBOUR. I think it's a complex issue, and I would like to continue to discuss it with staff, but I'm really not ready to give you my opinion on it, at this point.

Senator BILL NELSON. Thank you.

Commissioner LEIBOWITZ. Can I get back to you in a few days? [Laughter.]

Senator BILL NELSON. OK, the next goal. Ensuring that consumers are given rights regarding their information held by the data brokers, similar to the consumers rights that now exist under the Fair Credit Reporting Act. For example, the right to correct errors in that information.

Madam Chairman?

Chairman MAJORAS. It depends on the information in the particular database that the data broker is maintaining. So, for example, today, if the data broker is maintaining a database that contains consumer-reporting agencies' information used for credit eligibility or employment, for example, then, even today, yes, a data broker would be required to give that access. If it's a fraud database, on the other hand, giving a fraudster access to his or her information would defeat the purpose of the fraud database.

Commissioner SWINDLE. I could not have said it better.

Commissioner LEARY. I agree with the Chairman.

Commissioner HARBOUR. Like you, Senator, I am very concerned about the accuracy of information provided by the data brokers. I think that data brokers should adhere to best practices, possibly for accuracy, and it would be extremely worthwhile for leading industry and consumer groups to suggest possible best practices in this area.

Commissioner LEIBOWITZ. I agree with my colleagues. And I think you should think seriously about it.

Senator BILL NELSON. We've already discussed, I think, the Social Security situation. So, two more goals. Creating a blue-ribbon panel made up of industry and consumers to help develop best practices for safeguarding sensitive consumer information.

Madam Chairman?

Chairman MAJORAS. I confess, Senator, that I have not spent a lot of time thinking that through, but, in general, I am very supportive of self-regulatory-type efforts, and I'm very supportive of having the consumer groups and the industry groups talking to each other.

Commissioner SWINDLE. I cannot attest, with certainty, that they exist, but safe computing practices are everywhere. Devices, tools, technologies to protect data is everywhere. The problem is not so much the lack of it; it's the lack of implementation and deployment of it. As we all know, and several have reflected, people give away their Social Security number at just the drop of a hat. So, to get back to my point of a culture of security, we've got to change the way we think. It's not a lack of tools that is hurting us. It's not employing and thinking about those tools.

Commissioner LEARY. Senator, I think it's an ingenious idea, because it recognizes that what is adequate security is an ever-moving target, and technology is moving a lot faster than, at least, my ability to comprehend it. So, I think that having some people who are really adept at this, with various backgrounds, might be a very useful thing to do.

Commissioner HARBOUR. Senator, I think it's an excellent idea. Having industry, the privacy groups, the consumer groups come together and talk about this very complex issue would be an excellent way to proceed.

Commissioner LEIBOWITZ. I agree with my colleagues. It could be very, very useful.

Senator BILL NELSON. OK. And the final goal, fully funding a robust Office of Identity Theft within the FTC, with adequate resources to assist victims of identity theft.

Madam Chairman?

Chairman MAJORAS. Well, I've been known to say, Senator, that I don't think, in my 10-month tenure, I've ever turned down additional resources, so I thank you for that. But I will say, if the goal of that is—well, first of all, the FTC assists identity-theft victims today, and we will continue to do that. If what the legislation proposes, however, is that we would individually help each of the ten million identity-theft victims, that, I think, would be too much for any one agency to handle, particularly for ours, simply because identity theft is a crime, and we don't have criminal enforcement authority, so we're not involved in that aspect of prosecution.

Commissioner SWINDLE. Senator, I agree, certainly, with the Chairman's point about the crime being the issue here, but if I may run some numbers by us here today very quickly. We received roughly 250,000 identity-theft complaints in our complaint center this past 12 months, and I think it has been a fairly consistent figure. If we discounted half of those and said that, only 120,000 were really identity-theft problems, and if we took Senator Schumer's numbers—and I think he was referring to some survey, as I recall—of 175 hours to resolve that on the part of any individual—so, let's say it takes a month, and we have 120,000 legitimate claims—it takes a month to do this—that's one month's work out of one employee. The FTC, right now—I think we have about 1,100 or 1,200 employees——

Chairman MAJORAS. Eleven hundred.

Commissioner SWINDLE.—we would be required to have at least, using those numbers, another thousand employees. The FTC would then start to lose—well, well beyond losing its identity in its involvement with antitrust. We would become a completely transformed agency.

Now, I used half of the complaints to make the illustration here of what we're talking about when we throw this out, but there's a lot more to it than meets the eye. Remember, in the last 12 months there were approximately ten million people, supposedly, who were victims of identity theft. I'm talking about 120,000 resulting in the need to add 1,000 people in the agency. It's a very complex issue.

And, again, I will repeat it until I am blue in the face, even when I'm not a commissioner, that the first line of defense for everyone is the individual, himself, using good thinking about how he handles his financial and personal information.

Commissioner LEARY. Senator, I agree with my colleagues who have spoken thus far, and I just want to add a couple of thoughts for your consideration.

The skill set, if you will, and the capabilities to deal with identity theft vary tremendously. For example, a prosecutorial function aimed at getting the people who may have committed identity theft or facilitated it through negligence, one way or the other, is a very different function than counseling individual consumers as to how best to deal with their problem. And I think that, ultimately, this has to be handled on a decentralized basis, under common standards, to the extent possible.

Commissioner HARBOUR. I agree with the comments of my colleagues, but I would like to add a few other things.

The functions of the Office of Identity Theft, in my view, are already being fulfilled by the Federal Trade Commission. Currently, much of what you're seeking, as I said, I believe we're doing. We have victim assistance and counseling, we have a hotline, we have a toll-free number, we have extensive consumer education, we're the clearinghouse for all of the ID-theft victims, and we report on trends. As the Chairman indicated, individual representation would be extremely difficult. As I said, the Commission currently assists consumers. And what we do is, we educate them and we empower them. So, one of the best lines of defense, as Commissioner Swindle indicated, is educating them so that they will not become a victim of identity theft. And, also, if they are, then they know what steps to take to rectify it.

Commissioner LEIBOWITZ. Yes, I agree with the collective wisdom of my colleagues. I think, in your bill, you have a $60 million authorization. I think you'd probably have to put at least one more zero after that to make it actually work—to make it function and to not detract from the other missions of our agency.

The one other thing I wanted to mention, which is a common thread in all of the bills I've seen introduced, is civil penalties or fines. I think we all agree, on the Commission, that it is very important. It's a very useful deterrent. It'll make companies think twice before they violate the law.

Senator BILL NELSON. Thank you all.

Senator SMITH. Senator Burns?

Senator BURNS. When you go out and—and I would say that the collaboration of the industry coming together and using best practices for this, you—like Mr. Leary brought up—does bring up some of our own laws that, sort of, prevent that, because of antitrust and other exchange of information on the best practices, and all this. I'm wondering—and I'm coming down on the side of that anybody that collects information that doesn't have a license to do so is outside the law and should be shut down. I'm—maybe that's the only way we've got to doing it, but I think they have to have some reasonable license that gives them the guidelines to do business in this arena. And so, I'm coming down that——

But let's say that you go out, and you dealt with Microsoft and the other companies that you mentioned a little while ago for inadequate security systems. In other words, advertising, I would imagine, a system that assured the public that their privacy couldn't be—their information couldn't be breached, but then it didn't work. Is that a correct assumption on my part?

Chairman MAJORAS. On most of the cases we've brought, that is exactly what happened, yes.

Senator BURNS. OK. Now, when a person—say, you've got a breach here in some of these firms. Do you go out—do you actually ask them to explain their systems to you, and what actions they've taken, in order to protect the information that they might have stored?

Chairman MAJORAS. Absolutely. When we open an investigation under section 5, or under our Safeguards Rule, we do—we absolutely get behind what it is that a company has done to safeguard the information, and——

Senator BURNS. Would that be like Citicorp in this last——

Chairman MAJORAS. Well, we don't have jurisdiction over banks. That, obviously, is with the OCC and other banking agencies. So, we don't—we aren't—we do not investigate all of the breaches that you've heard about. We are investigating some.

Senator BURNS. Well, where I'm going here—and, Mr. Swindle, I think we've had this discussion before—do you have the people and the expertise to go out to a commercial organization and collect the information on the system that they use, and make a judgment whether it's adequate or not?

Commissioner SWINDLE. Yes, sir. We have highly qualified investigators. I think the limitation that the Chairman was referring to is, we just don't have jurisdiction over the banking industry; it's covered under a different jurisdiction. But we have incredibly competent investigators that have got, literally, years of experience, and we know how to do this.

Senator BURNS. Are you looking at these organizations that were in our briefing here? And did you look at their systems and determine that they had adequate security systems?

Chairman MAJORAS. It depends on which ones you're talking about. I mentioned a couple in which we actually did bring cases, and we did——

Senator BURNS. Well, let's go—let's go—here, we've got Boston College.

Chairman MAJORAS. I'm sorry, Senator, I'm afraid I can't comment on——

Senator BURNS. OK. Well, I——

Chairman MAJORAS.—non-public investigations.

Senator BURNS.—and we shouldn't——

Chairman MAJORAS. So, I apologize.

Senator BURNS.—do that, either.

Chairman MAJORAS. Right.

Senator BURNS. We don't do that, either. But I guess that's where I'm going, that—and are we looking at them before something happens, or after something happens? Do you have the authority to monitor and advise that their system might not be adequate for information protection?

Chairman MAJORAS. We don't have regulatory authority in the same way, for example, that the banking agencies closely regulate the banks. So, we don't have an ongoing dialogue, for example, with various industries on what their security measures are that they have in place.

Obviously, yes, we can enforce, if we learn that they don't have adequate security in place. And, unfortunately, sometimes the way we learn it is when there has been a breach. But we don't need a breach in order to find that reasonable security measures have not been taken, in violation of section 5 or GLB.

Commissioner SWINDLE. Senator, if I may interject, we've had a couple of cases, in which we've been told by others who watch, perhaps, more carefully than we do, because it's their primary focus—we do a lot of antitrust work and other things—but where we receive complaints, it has caused us to go make inquiries. We don't, as a routine matter, audit anybody, in the sense that the banking regulators might conduct, if that's the right word, an audit. But we do look at things.

And, Mr. Chairman, I hate to leave this discussion—because, as I said, I have a passion for all of this—but, as I mentioned to you, I have a plane to catch. And I would just say to you all, once again, it has been an absolute honor to work with you. And I bid you adieu, and I'll probably be around somewhere.

Senator SMITH. Thank you so much.

Senator BURNS. Keep your name in the phone book—we may need you one of these days—would you?

Commissioner SWINDLE. I'm putting everything on the Do Not Call List, sir.

[Laughter.]

[Applause.]

Senator BURNS. I guess in that line of questioning, I'm driving toward prevention, actions that we can take. And I think Senator Nelson is, kind of, on target that it's going to take an industry—the industry has to drive this, rather than any kind of a regulatory regime that we could put in place. Am I not correct on that?

Chairman MAJORAS. Well, I mean, I do think—I do think it would be—it's extremely helpful for industry and—to help drive this, Senator, because we can't be the eyes and ears within every——

Senator BURNS. Yes.

Chairman MAJORAS.—company, in terms of what they're doing. And that's why we like our flexible and broad Safeguards Rule, because it says to companies, hey, you have to put in place appropriate procedures, depending on the kinds of information you have and the kinds of business you have, and so forth, and depending on what technology, for example, is available to you today—and fives years from now, it's different—in order to not run afoul of the law.

Senator BURNS. The way technology's moving, next week it's going to be different.

Chairman MAJORAS. Absolutely. And we want companies to take that into account.

Senator BURNS. But it's kind of like trying to put your thumb on JELL–O; I mean, it just moves, but that's the direction I'm going, I think, is prevention more than anything else, and then very strict fines. I agree with Mr. Leibowitz, I don't think you can make a fine too high for this kind of activity.

I thank the Chairman. I'm sorry I ran over my time. And thank you for coming today. We appreciate that very much.

Senator SMITH. Senator Ben Nelson?

Senator BEN NELSON. Thank you, Mr. Chairman. And I, too, thank the witnesses for helping enlighten us as we work our way through this challenging issue.

I asked Attorney General Sorrell if he thought that there was a way to square the challenge that you have of dealing with states interested in this area, together with the Federal interest. Is there a way to harmonize it? Recognizing that the states do a great job at consumer protection, dealing at the closest level with the residents is an important factor for us to all consider. The closer it gets to Washington, except for people in the area, the more removed it is from folks out in the Midwest and on the West Coast.

Recognizing all that, in trying to—are you suggesting, Ms. Majoras, that it's an either/or situation? Either—as it relates to the standard? Either the Federal Government does it or the states do it; otherwise, you get the patchwork quilt problem, compliance, or companies will ignore whatever the Federal standard is, if it's a floor, and go to the highest level established by the states, because they don't want to have to deal with individual differences between and among the various states?

Chairman MAJORAS. Thank you, Senator.

First, I want to make sure I make absolutely clear that I agree with you wholeheartedly that the states are tremendous enforcers of consumer-protection laws, and we do—we do need their help, and we work effectively with them. And, in this space, we do believe that state AGs must be able to enforce.

My only point was a practical one. It's not philosophical; it's simply practical. You could work very, very hard on a standard, and try to come up with the perfect standard, but if you say it's a floor, I'm just not sure that—and perhaps my colleagues would like to comment—I'm not sure that it will be meaningful, in the end, if other states enact higher standards. States will automatically have to go to the higher standard, in running their business. So, it just depends on how you feel about that.

Commissioner LEIBOWITZ. I'd just say that, for some things, like a standard for notification, preemption seems to make a lot of sense. On the other hand——

Senator BEN NELSON. That's what I was thinking——

Commissioner LEIBOWITZ.—on the other hand, states are wonderful laboratories for experimentation. They have been for as long as—as long as there have been states. And so, for something like a credit freeze, which California is experimenting with, or Vermont's experimenting with, it may make sense to let them continue to do so. You wouldn't have to preempt in that area.

Senator BEN NELSON. Well, that—you're anticipating where I was going with the laboratories of democracy. I think Jefferson was, in fact, right; and, in fact, we have seen great things come from the states. Am I right to say that the states moved on this before the Federal Government did?

Chairman MAJORAS. On the notice requirement——

Senator BEN NELSON. On the——

Chairman MAJORAS.—they did.

Senator BEN NELSON.—notice requirement, yes.

Chairman MAJORAS. Yes.

Senator BEN NELSON. So, there is a concern, I would have, that we not put into place a standard that would become, if you will, a fixed standard, where there's no further experimentation. It's one of the concerns I have when we take the best practices of the states, and we put them into place at the Federal level, and say, "OK, we've solved that." But, when we do that, we tend to stop experimentation, and things remain static, rather than dynamic. I'm hopeful that there would be a way to work through this, to where we permit the states to continue to do the experimentation. We don't stop commerce. We don't in any way impede the ability of commerce to move forward on this, but yet we protect the public.

With the former Attorney General sitting next to me, I can say that many of the Attorney Generals don't think that AG stands for Aspiring Governor. And so, they——

[Laughter.]

Senator BEN NELSON.—so, they take—they take great care—as a former Governor, I used to have to be concerned about that.

[Laughter.]

Senator BEN NELSON. As they continue to work to bring about protections of the consumers at the local level, they continue to do a great job, and I would hate to see anything that would get in the way, block, or would in any way impede their ability to continue to do that. I'd like to get your thoughts about that.

Commissioner HARBOUR. Senator, we've had this discussion within the Commission. And I know the Chairman says she takes a practical view. We've also discussed the philosophical view. And everyone does love the dissenting opinion of Brandeis, where he said one of the happy incidents of state—the Federal system was that states may serve as a laboratory and try novel social and economic experiments without risk to the rest of the country. But I think whatever approach is chosen by Congress, I believe that state attorney-general enforcement is essential.

Senator BEN NELSON. I don't think we're—this isn't a challenge. It's the equivalent of squaring a circle. But it's going to be a very delicate area to carve out the relationship so that we get the best of both, so that we end up with the best practices; because, after all, that's what the consumers are expecting, and that's what they need; and they deserve it, as well.

Well, thank you, Mr. Chairman, for the hearing.

Thank you very much.

Senator SMITH. Thank you, Senator Nelson.

Senator Pryor?

Senator PRYOR. Thank you, Mr. Chairman. Was Senator Allen next?

Senator SMITH. On my list, you got here before he did.

Senator PRYOR. OK. Thank you, Mr. Chairman. And I want to thank you, again, for this hearing. I know a number of our colleagues have thanked you, as well, but we really appreciate your leadership on this and other issues.

Ms. Harbour, let me start with you, if I may, and that is, you mentioned, in your opening statement, Social Security numbers. And, as I understand what you said—maybe I misunderstood it, but as I understand what you said, you said that, basically, data brokers should not be allowed to share Social Security numbers, except within fairly narrow parameters. Do I have that right?

Commissioner HARBOUR. Well, what I had in mind, Senator—I think Congress should consider imposing stricter controls on the sale, distribution, and use of Social Security numbers, and that perhaps Congress should consider breaking the habit of industry using Social Security numbers as authenticators. But I also appreciate all of the very thoughtful comments that my colleague, Commissioner Leary, indicated, as well. It's a very complex area, and it's going to take a very delicate balance between the right to privacy and the right to information and the economic factors that go into the importance of Social Security numbers.

Senator PRYOR. I agree, it's complicated, and it's not an easy fix, just a one—one simple solution isn't there, probably.

Let me ask this, while I have you, on the subject of Social Security numbers. Is it your view that Congress needs to act to restrict Social Security numbers, or does the FTC have the authority right now to implement a regulation?

Commissioner LEARY. Well, Senator, the FTC has the essential authority to attack people for unfairness or deception if they misrepresent what they are going to do with information that they collect, or if they misrepresent the security with which they would treat it. But, in general, we do not have the authority to say to any particular institution that, "You shall not transmit it," other than authority specifically granted to us under Gramm-Leach-Bliley or Fair Credit Reporting Act. We do not have a free-roving authority to regulate it——

Senator PRYOR. That's my sense——

Commissioner LEARY.—in that area.

Senator PRYOR.—of it, as well.

Chairman MAJORAS. Right.

Senator PRYOR. Yes.

Chairman MAJORAS. Right. I was just going to add that, under Gramm-Leach-Bliley today, if a Social Security number has come from a financial institution, then there are some restrictions on the transfer of that Social Security number. And to the extent that we have jurisdiction to enforce GLB, we do have that piece. But we don't have a general—we don't have general rulemaking authority in this area.

Senator PRYOR. While we're on the subject of Gramm-Leach-Bliley, I'm curious for your thoughts—and, Ms. Majoras, maybe we'll start with you—on how Gramm-Leach-Bliley is working, from your standpoint and given the focus you have on it. How's it working? And, also, I know that there has been some ideas floated here about the Safeguard Rules in Gramm-Leach-Bliley, and how that interfaces with privacy, and how we should proceed into the future, and whether maybe we should expand a little bit on Gramm-Leach-Bliley, et cetera. So, I'd just like to get your thoughts on that.

Chairman MAJORAS. Thank you.

Gramm-Leach-Bliley, of course, is enforced by several different agencies in the FTC. You know, the banking agencies, for example, enforce against those financial institutions and the like, and the FTC has whatever's left when you take those regulatory agencies out of it. We do think that the Safeguards Rules under it are working appropriately. There have been questions raised about whether—under the privacy provisions, whether the notice to consumers has been working very well. We don't have exact numbers, but understand that consumers have not responded well to those notices, that most have gone into the trash can, as opposed to being read. And we are actually working now with industry to see whether there's something that could be done with those notices to make them more consumer-friendly, if you will.

Senator PRYOR. Let me interrupt just right there. So, do you have the empirical data on that? Or is that what you're trying to collect?

Chairman MAJORAS. We don't have empirical data today. I don't have exact numbers for you.

With respect to extending the Safeguards Rule, the Safeguards Rule is broad and flexible enough, I think, to be applied beyond financial institutions, in GLB, to other businesses that collect and hold sensitive consumer information. And we think that would be—that that is a good extension, that rule, if Congress sees fit.

Commissioner LEIBOWITZ. I agree with the Chairman.

Commissioner LEARY. Senator, I agree with the Chairman. I'd just add, if it's not obvious, that Gramm-Leach-Bliley is a classic illustration of the risks that you might encounter with excessive notification. We're all bombarded with notices and documents of various kinds, and, if there are just too many, the message gets lost. For example, there might be some theoretical compromise of your data, however limited. If every time you automatically get a notice—eventually, it's like the boy who cried wolf, in the old fairytale, you stop paying attention.

Senator PRYOR. My sense is that there are a lot of people in this country that are just tuning them out. You know, maybe the first couple of times they got a notice they got read. And, you just get enough of them, you just start to tune it out, they start to lose——

Commissioner LEARY. Yes.

Senator PRYOR.—their impact.

Commissioner LEARY. Right.

Senator PRYOR. Mr. Chairman, that's all I have. Thank you.

Senator SMITH. Thanks, Senator Pryor.

Senator Allen?

Senator ALLEN. Thank you, Mr. Chairman.

Let me just make some prefacing remarks before I ask for your insight.

The states are laboratories. Having been Governor, I think the states come up with better ideas and are more responsive to the needs and values of the people than is the Federal Government. However, the states did create the Federal Government, and our present Constitution is one in which we wanted to make sure that there was a free flow of interstate commerce. And if the states are doing something that is harmful to interstate commerce, we don't want to be allowing that.

I look at this situation as akin to other areas, where, actually, the states and the attorney generals are partners, we're not in competition. But we—it's a national security standard that we're concerned with. A lot—we get into privacy, but this is more of a security issue, of information, data, and identity, than it is a privacy issue. But the way it ought to work—like in many other areas, everything from OSHA to mining laws to even bank robbery—those are all tried in Federal court, but most of the time it's local law enforcement, or maybe a state police officer, who has apprehended the bank robber. So, I think the FTC, obviously, is preeminent, but I think, as the Chairman said, Chairman Majoras, this is one where we do want to work with the states.

My view of this is that we should have uniform national security standards. We do need to make sure information of consumers is protected. If there's a breach, we've got to figure out what circumstances should a custodian notify the affected citizen where they reside.

Now, since we have all of you here, if—the question really, for me, is, if the FTC—and you do have authority to bring actions against these companies that fail to adequately safeguard consumer information. In your testimony, you said you have the Federal laws. Now, as a follow-up on this, if the FTC has sufficient authority to bring enforcement actions against so many companies, can you identify any gaps—any gaps in your authority—where you would recommend—not just saying, "Well, it's financial institutions," and so forth—but are there any gaps where you would recommend that we, as a Congress, grant you all, with the Federal Trade Commission, further enforcement authority?

Chairman MAJORAS. Thank you, Senator Allen.

One gap that could be filled is the extension of our GLB Safeguards Rule to other businesses. It's a fair question to ask why—if we can already bring these cases under section 5, why would we need that? But if you take, for example, the BJ's case, and our unfairness standard that we used in bringing this case, today, that requires, first and foremost, that we prove substantial consumer harm. And, of course, what we would prefer is not to have to wait until substantial consumer harm is shown all the time; in other words, to have companies recognizing that putting in place reasonable security measures is what they should be doing under the law, because what we most want to do is prevent the breaches. And then, of course, you've pointed out the notice provisions; and, as of today, of course, there is no Federal notice law, Senator.

Senator ALLEN. Restate that again. Extension of what, specifically? I want to make this very——

Chairman MAJORAS. OK.

Senator ALLEN.—clear——

Chairman MAJORAS. OK.

Senator ALLEN.—for all of us.

Chairman MAJORAS. All right. The FTC's Gramm-Leach-Bliley Safeguards Rule.

Senator ALLEN. All right. Now, if you had had such additional enforcement authority—and you mentioned one particular case which you can't talk about—if you had this enforcement authority at the beginning of this year, would you have prevented the breaches that we've seen since January of this year? And, if not, are we merely talking about how much we can fine a company for failure to act responsibly?

Chairman MAJORAS. Well, I'm not sure that, with respect to any specific breach, we could have prevented it. And, of course, we're investigating some of them; and so, we'll learn more information. But I do absolutely agree with Commissioner Swindle that what we need to do is create a culture of security in business. Businesses would not, of course, treat packages with cash in them in a way in which that cash could be stolen easily. And so, I think if the law is in place, and it is adaptable to all manner of businesses, the industry will likely respond to that. And there is no such thing as perfect security, Senator. We know that with respect to national security, and in all instances. But I do think that it will get companies, who have not brought up to date their security procedures, thinking, "Gosh, now it's law, and we must do this."

Commissioner LEARY. Senator, let me just expand on that a minute——

Senator ALLEN. Yes, Commissioner Leary.

Commissioner LEARY.—because I agree with it completely. The mere fact that businesses are on notice, that they are now subject to a specific legal requirement that they were not specifically subject to before, will induce a level of compliance, because most businesses are law compliant. The prime enforcers of law in the United States are not people sitting on this side of the table, but people who are counselors to businesses, who say to them—to their clients—that, "Now we have a legal requirement, and we'd better set up procedures to be in compliance with this, because you might get sued someday down the road."

Senator ALLEN. Thank you.

Commissioner LEIBOWITZ. I agree with my colleagues. Let me just add one point, which is: a useful gap that could be plugged would be in the cross-border fraud area. We just don't have the authority, often, to receive information from our foreign law enforcement counterparts. And if we can get that ability, we'll be able to more effectively go after malefactors who are doing bad things to Americans from abroad. By the way, that's not just in the context of data security; it's also in the context of spam, spyware and——

Senator ALLEN. Right.

Commissioner LEIBOWITZ.—various other problems.

Senator ALLEN. Well, Mr. Chairman, we were actually working on that. That was one of the key components, on the spyware.

Thank you, Mr. Leibowitz. We'll make sure any legislation gives whatever assistance in that regard to you all. Thank you.

Ms. Harbour?

Commissioner HARBOUR. And just to put a fine point on what Commissioner Leibowitz said, with the ChoicePoint data breach, as I recall, the information was given out to a Nigerian national. And had we had the cross-border legislation, that might have enabled us to share information with other countries, and perhaps have facilitated an investigation, or perhaps prevented something like that from happening in the future.

Commissioner LEIBOWITZ. One more thing to add, which is, civil penalties or fines would be useful, too, in the context of——

Senator ALLEN. Additional civil——

Commissioner LEIBOWITZ.—this legislation.

Senator ALLEN.—higher civil fines and penalties.

Mr. Chairman, thank you.

Thank you all. In the event that we craft legislation, as far as I'm concerned, you gave me the good framework for it, and I very much appreciate it. And we want to make sure that you all can do your job protecting our consumers in this country, and, obviously, working with international counterparts, as well. But thank you.

And thank you, Mr. Chairman.

Senator SMITH. Any more questions?

Senator ALLEN. No, I don't have anything further.

Senator SMITH. Thank you, Senator Allen.

Commissioners, the FTC, itself, has documented the difficulty that peer-to-peer users have when they use software programs. They can unwittingly share their tax returns, bank account numbers, credit cards, medical records, resumes, e-mail in-boxes, and legal documents of all kinds, with literally millions of people. The question I have is, Do you have any suggestions on how we can better educate consumers about the ongoing risks of identity theft and fraud on P2P networks?

Chairman MAJORAS. Well, thank you, Senator. It's an excellent question, and it's something that we, at the FTC, have been working on. We have materials designed to educate consumers. But what we are—what we have been doing is working with the peer-to-peer file-sharing industry, because we think that, to the extent that consumers need to be warned of risks, if they can be warned the minute they pull up the—download the software or begin working on the P2P file-sharing program, that really is the best place. And in—when we first started this, last year, after we had our peer-to-peer file-sharing workshop—at which we were pleased to have you as a speaker, Senator—really, almost none of the file-sharing companies had disclosures and warnings on their software. And, today, that has changed a great deal. I can't tell you that that's absolutely going to be enough, but we have been focusing a lot of efforts in that area.

Senator SMITH. If it isn't enough, do you need more tools from us?

Chairman MAJORAS. We are—I think, Senator, we'd like the opportunity to finish what we're doing now, and then have the opportunity to come back to you and talk to you, if we think further tools are needed.

Senator SMITH. OK.

Chairman MAJORAS. And, of course, the Supreme Court's decision in Grokster may also give us some guidance.

Senator ALLEN. Yes.

Commissioner HARBOUR. If I might just add to what the Chairman indicated, the Commission staff intends to continue to encourage the development of best practices with regard to the risk disclosures, but also the risk of inadvertent file sharing appears to have decreased, due to technological measures adopted by some of the peer-to-peer applications, although the risk of inadvertent file sharing may vary, depending on what the application is. I think there are new technological developments that are coming onto the market that are protecting consumers.

Senator SMITH. Is the European Union—or Japan or other nations, are they running into these issues, as well? And do you have any—do you do any work with them across the ocean?

Chairman MAJORAS. We do, Senator. In fact, a great deal of work with them across the ocean. The EU has a much broader privacy and security scheme in place, as opposed to going after areas in which there's harm. It's a very broad, comprehensive—indeed, it's so broad that, when I recently, on behalf of the Commission, attended the annual meeting of the International Competition Network, we weren't allowed to have a list of who was attending, because that might violate the privacy rights of the folks who were actually in attendance. In Japan, I've had folks go to conferences, where they're not—no one is given a name tag, because, if someone wore a name tag, that might violate privacy rights—so, in fact, there are broader schemes out there with other countries. We do work very closely, through several international organizations, and on a bilateral basis, to share what has worked and what has not worked.

Senator SMITH. Do you need any more tools in dealing with these other nations? Do you have what you need now?

Chairman MAJORAS. Well, we have, in the cross-border fraud legislation that we have promoted, there is some language in there that would give us some more funding to be able to work more closely with our counterparts in this space, which is becoming so important to our work, as you know.

Senator SMITH. Well, it's clearly a problem that doesn't know borders, so I want to say that for the record. And we appreciate what you're doing internationally.

I want to bring to your attention a constituent's problem of mine. A constituent in Eugene, Oregon, contacted the Oregon Department of Justice, filed a fraud report. Last year, she had been a victim of identity theft, after which she filed a fraud alert with her credit union, filed a police report, put a fraud alert on her credit report, yet this same individual was revictimized a year later. And I'm wondering, What do you say to consumers who do everything right to protect themselves, and yet still fall prey to identity theft?

Chairman MAJORAS. Well, we say we're working as hard as we possibly can to make sure that that doesn't happen again, and to make sure that it doesn't happen to additional consumers.

One of the things that we do—I commented on the fact, Senator, that identity theft is a crime. And that means that it's prosecuted, most often, except in very large national or international rings, at the very local level. And so, one of the things that we try to do is train local police officers. We have a very big program with the Association of Police Chiefs to try to train those who are on the ground dealing with these consumers at the time. And I'll let my colleagues weigh in here, as well, if they wish.

Commissioner LEIBOWITZ. We're a consensus-driven organization. [Laughter.]

Senator SMITH. I want to highlight a comment I made earlier, and I do this in conclusion to our hearing today. I have in front of me an article from the *MSNBC.com* website, and it highlights the connection between ID theft and methamphetamines. There was, in Eugene, Oregon, again, an ID-theft ring that—their ring bosses use meth addiction to keep their runners in line and to get new recruits. In the case of Steven Massey, convicted for his role as a ringleader of an ID-theft gang in 2000, methamphetamine was the glue that kept this guy's ring together. Massey knew where to find meth addicts, and he made them a simple proposal. Said he, "I'll trade mail for meth." Soon, he had an army of meth addicts prowling the neighborhoods near Eugene, stealing mail out of hundreds of mailboxes, and raiding the local recycling center, for pre-approved credit-card applications. Others in the ring broke into cars to steal purses and wallets, not for money, but for ID papers. By the time Massey was arrested, investigators say he had gained access to over 400 credit-card accounts and netted close to $400,000. He eventually pleaded guilty to conspiracy to commit computer fraud, and to mail theft. It's a typical case in Oregon. "Ninety percent of our ID-theft cases deal with drugs," said the local policemen, "and it's usually methamphetamine, which is easy and cheap to produce in mass quantities."

I highlight this, not to bring attention to my state, because I think it's a problem being experienced very broadly in this country, but I do this only to let people know just how dangerous this is. These are very dangerous people, and, obviously, one of the most unsurly of trades in illegal drugs.

I don't know whether you would care to respond to that—yes, Ms. Harbour?

Commissioner HARBOUR. I know that crystal meth is a very serious and complicated problem. I do know that Senator Cantwell was concerned that the use of crystal meth in the State of Washington was fueling identity theft, as well. And I know that she had worked very hard to get local law enforcers in her state to take the issue very seriously; and, in fact, had involved Representative David Reichert, the former King County Sheriff, who, by the way, captured the Green River serial killer. But, anyway, local law enforcers are on the front lines, and I know that they're dealing with problems related to both drug use and identity-theft victims. At the Federal Trade Commission, obviously, we have no criminal law enforcement jurisdiction. The expertise of dedicated on-the-ground local law enforcers is irreplaceable. So, I suppose I would urge all of the Senators and the Congressmen to use some—to convince your state and local enforcers to really take a look at this issue, and to take this seriously and step up to the plate.

Senator SMITH. Thank you very much.

I'm going to ask unanimous consent—I guess I'm alone, so I agree——

[Laughter.]

Senator SMITH.—to include in the Senate record a statement from Oregon's Attorney General, Hardy Myers, that it speaks to this whole issue and the connection of identity theft and drugs, specifically methamphetamine.

[The information referred to follows:]

PREPARED STATEMENT OF HON. HARDY MYERS, ATTORNEY GENERAL OF OREGON

Police investigating identity theft crimes are becoming increasingly aware that the perpetrators are almost always users of methamphetamines. Oregon has an especially high rate of Identity Theft (9th in the Nation) and has the largest number of citizens in meth treatment programs of any state in the country. Both of these dubious distinctions lend themselves to one another. Meth users are many times recruited by leaders of ID theft rings to steal personal information from their victims.

The meth users, in turn, are given drugs as payment by the leader of the ID-theft ring.

IDs are especially easy to get in Oregon—in fact, Oregon ranks 48th out of 50 states in the ease of acquiring identification. Currently, for example, the DMV has approximately 6 million active Oregon driver's licenses on file, yet there are only 3.5 million residents in Oregon. In once instance, the Marion County Sheriff's Office shared one case in which an individual secured 20 DMV issued licenses within a 5-hour period.

There are many reasons that identity theft seems to be so inexorably tied to meth use. Meth users, by virtue of their addiction, go on binges in which they are awake and focused for days at a time. Consequently, they must spend days at a time sleeping off the consequences of their actions. This means that part-time jobs are difficult to hold. As meth is an expensive habit to maintain, sources of income are needed to obtain the drug. Furthermore, according to a professor at SJSU in San Jose, meth's "unique psychopharmacological properties would assist ID theft—the whole detail-oriented aspect of it, the obsessive-compulsive aspect of it."

Identity theft lends itself well to this because it can reap large monetary benefits, with relatively smaller punishments. As a police detective in Eugene put it, "they (meth users) can make more money in a fraud crime than they can sticking a gun in someone's face. If you bring a gun in a bank, you can face life in prison. Or you can write a series of bad checks and score 10 times that amount and just get parole."

There seems to be no official data that states the percentage of ID-theft crimes that are connected to meth. The estimations vary—but typically officials say between 85–95 percent of all ID theft crimes are in some way connected to methamphetamine. In 2003, 100 percent of identity theft case worked by the Fraud and Identify Theft Enforcement Team investigators in Washington County, Oregon had a methamphetamine nexus.

There have been many documented cases in which a meth users has been caught with a number of identifications, financial records, and Social Security numbers. In one example in Tualatin Oregon, officers located 340 separate probable victim identities in a storage unit along with a boxed up meth lab that only needed a few components to start cooking again. Of the 1,240 separate identities, there was identify information in the form of full profiles of persons, checks, ID cards, credit applications, W2's tax information, and much more.

Oregon, by virtue of being among the most ravaged of states by both identity theft and methamphetamine, can be a unique example of the connection between the two. ID theft affects thousands of Oregonians every year, and it is being perpetuated by users of methamphetamine.

Senator SMITH. Let me just say how appreciative we are of your presence here today, the contribution you've made. We look forward to working with you to make sure you have the powers and authorities necessary to get ahead of what is a burgeoning problem in our country. We've got to protect our consumers from this; and, clearly, new tools are called for. And your input is valued, and will be included. And we look forward to working with you as this legislation develops. And, most of all, thank you for your public service.

Chairman MAJORAS. Thank you, Mr. Chairman.

Senator SMITH. We're adjourned.

[Whereupon, at 12:15 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

North Dakota is first in the Nation in many good respects. But I am happy to say that North Dakota ranks 49th in the Nation in the number of ID theft cases, on a per-capita basis. There are almost five times as many cases of ID theft in Arizona, on a per capita basis, than in North Dakota.

Still, even though we have had relatively few cases in North Dakota, the first-hand stories of North Dakota victims are certainly devastating ones. This is clearly a national epidemic. And I am particularly worried about the many instances in which data brokers have lost the sensitive financial records of hundreds of thousands of Americans.

I am a co-sponsor of S. 768, the Comprehensive Identity Theft Prevention Act, which my colleague Senator Nelson (along with Senator Schumer) has introduced.

This bill does a number of things:

- It bans unregulated commercial trading of Social Security numbers, and prohibits commercial entities from asking individuals for their Social Security numbers, unless no other alternative identifier that can be used.
- It establishes an Office of Identity Theft within the Federal Trade Commission (FTC), as a "one stop shop" to help the millions of victims of identity theft each year restore their identities. This office would also be responsible for passing regulations to protect consumers' sensitive personal information that is collected, maintained, sold, or transferred by commercial entities. It would have the authority to bring enforcement actions for violators of the regulations.
- It requires safeguard rules for all commercial entities: companies must take "reasonable steps" to protect all sensitive personal information that they store.
- It requires information brokers subject to full regulations by the FTC; and consumers would be afforded the rights they have under the Fair Credit Reporting Act regarding credit bureaus.
- It requires breach notification: all commercial entities must notify individuals when there has been a breach of the individual's sensitive personal information.

I am particularly concerned about the pervasive use of Social Security numbers by businesses as a means of identifying potential customers. I believe that the use of misappropriated Social Security numbers is one of the main accelerants that fuels the epidemic of ID theft. I know that many businesses will argue that they need Social Security numbers to distinguish one customer from another. But the Better Business Bureau estimates that there were 9.3 million victims of identity theft in 2004. Clearly, there are competing interests here—and given the number of victims, I think we need to provide much more protection for the confidentiality of Social Security numbers.

When a company like LexisNexis is hacked into, and thieves steal the personal data of 310,000 Americans—including not only their Social Security numbers, but even the date and location where the Social Security card was issued—it is clear that we have a serious problem on our hands.

I have read through FTC testimony. It states that "private and public entities routinely have used Social Security numbers for many years to access their voluminous records," and suggests that the solution is not to restrict the use of Social Security numbers, but rather to go after those who use Social Security numbers for criminal purposes. I am certainly in favor of going after the bad guys, but I think we also need to restrict the use of Social Security numbers far beyond the status quo.

So I look forward to discussing this point with the other commissioners today.

I am also interested to hear from Vermont Attorney General William Sorrell on whether Federal legislation on the issue of ID theft should create a ceiling that preempts recently enacted state laws in this area. North Dakota is one of the states that has recently passed legislation requiring notification of individuals when their personal data has been compromised. I am not sure that we want to be capping the efforts of states to protect individuals from ID theft. The bill that I have co-sponsored with Senator Nelson does not do that.

With that, I thank the witnesses for attending today.

PREPARED STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Mr. Chairman, thank you for calling this hearing on the vitally important issue of identity theft. I commend you for making this issue a top priority.

As you know, I am a strong and vocal proponent of privacy protection—especially with regard to the distribution of personal information that can lead to the physical, financial, or psychological harm of an individual if the information falls into the wrong hands.

In 1994, after an actress in my state was murdered by a stalker who obtained personal information about her from the Department of Motor Vehicles, I authored the Driver's Privacy Protection Act to keep personal information held by a state Department of Motor Vehicles from being released without the consent of the individual. The Supreme Court upheld this law on a unanimous 9–0 vote.

That was during the days of the Internet's infancy. While the Internet has done wonderful things, it—and the computerization of more and more data—is making it easier for identity thieves.

The Privacy Rights Clearinghouse, a nonprofit group in San Diego, estimates that nearly 4 million people's identities have been compromised through means such as hacking, dishonest insiders, and computer theft since mid-February. This number does not even include 5 million people whose sensitive information is on the backup tapes lost by Bank of America and CitiFinancial.

According to a 2003 FTC study, over a period of 1 year, nearly 10 million Americans were victims of identity theft. Losses to business and financial institutions were nearly $48 billion and consumer victims reported an additional $5 billion in out-of-pocket expenses.

Criminals use misappropriated and stolen consumer information to assume the identity of innocent individuals. They get credit cards and mortgages in someone else's name and even use an assumed identity if caught committing a crime. The identity thieves then disappear and it is the victim who is left answering the calls of debt collectors and the police.

Data brokers are of particular concern when it comes to identity theft. These companies actively collect and sell information about individuals.

As aggregators of sensitive information, data brokers are attractive targets for identity thieves. And, unfortunately, the last few months have shown that criminals are succeeding in stealing information from them.

Since the beginning of the year, we have learned that breaches of security at ChoicePoint and LexisNexis have resulted in information on approximately 145,000 individuals in ChoicePoint's case and 300,000 records in LexisNexis's case being exposed.

What is worse is if this had happened a few years ago, we might not have even known about them. It is only since a California credit law went into effect in mid-2003 that companies have been forced to notify Californians when their confidential information has been compromised. That required notification to California's consumers has resulted in the whole country knowing about these thefts. But, outside of California, people do not have a right to know when their own personal data may be compromised.

This must change. People have a right to know when they are at risk. They have a right to know before they get turned down for a loan because someone else ruined their credit record. They have a right to know before they are arrested for someone else's crime. We, however, should not focus solely on data brokers. Many other organizations routinely store sensitive personal information. In April, DSW—the shoe store—admitted that its computer system had been hacked allowing criminals access to the credit card and driver's license numbers of approximately 1.4 million customers.

Identity theft also raises serious homeland security concerns. Terrorists, too, are able to use sensitive consumer information to assume false identities. Unlike criminals, however, terrorists will avoid the activities that normally alert a person to the fact their identity was stolen. So long as the terrorist pays the credit card bills, it could be years before the deception is revealed.

Legislation is needed to address the consumer harm and security threat arising from identity theft. Therefore, I have cosponsored the Comprehensive Identity Theft Prevention Act (S. 768).

The legislation would create and fund the Office of Identity Theft in the FTC and create an Assistant Secretary for Cyber Security in the Department of Homeland Security.

Moreover, it would regulate data brokers and ensure that companies maintaining sensitive personal information protect that data. A notice provision based on California's law would require companies to inform affected individuals of security breaches and give those consumers additional rights to protect their sensitive information.

This legislation is timely and necessary. I look forward to working with my colleagues on this Committee to move the bill forward.

I thank you again, Mr. Chairman.

PREPARED STATEMENT OF FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Mr. Chairman,

Thank you for holding this important second hearing on the compilation, storage, and sale of sensitive personal information, and the American public's increasing concern and susceptibility to identity theft.

Whereas our focus in May was to look at the *actors* in the data brokerage industry, today we focus on what the Federal Trade Commission is doing to help combat identity theft and what *Congress* can and should do to combat this increasing threat.

Recent security breaches at the Nation's largest data brokerage firms have left millions of Americans vulnerable to identity theft and scams. Overall, some 10 million Americans were victimized by identity thieves last year.

And the situation is only getting worse. The year 2005 has brought news of one security breach after another, with no end in sight. Some of these breaches have been high-tech, resulting from improperly or illegally accessed passwords. Others have been caused by mere carelessness, sometimes during the transport of files or disks.

Regardless of method, these breaches have exposed sensitive personal information about millions of Americans in the past year alone. This is simply unacceptable, and it warrants our attention.

In the wrong hands, an individual's private data can wreak havoc on a victim's life—ruining their finances and credit rating, their ability to obtain a mortgage, and often their *good name.*

Victims of identity theft often spend years and large amounts of money to repair the damage done by identity thieves.

Advances in technology allow more information to be compiled faster and in fewer databases. The collection and storage of personal information is a big business, and now is the time to exercise better oversight of this problem and consider how we can play a role in protecting Americans from identity theft.

Mr. Chairman, our laws must ensure that companies protect personal information with great care.

We must work harder to protect Social Security numbers. Social Security numbers should be requested and given based on *need.* Furthermore, we must make sure Americans are aware of how and when their Social Security number is being used.

We must also *notify* consumers when a breach has occurred that puts them at risk of identity theft.

I'm interested to hear from the Federal Trade Commissioners on what efforts the FTC currently employs to protect Americans, and what their agency is prepared to do moving forward to help combat identity theft.

Thank you, Mr. Chairman.

○