AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING CONSUMERS' DATA: POLICY ISSUES RAISED BY CHOICEPOINT

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MARCH 15, 2005

Serial No. 109–76

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

99–916PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

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

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
JAMES D. BARNETTE, *Deputy Staff Director and General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

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

JAN SCHAKOWSKY, Illinois
Ranking Member
MIKE ROSS, Arkansas
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
BOBBY L. RUSH, Illinois
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan, (Ex Officio)

CONTENTS

	Page
Testimony of:	
Majoras, Deborah Platt, Chairman, Federal Trade Commission	17
Sanford, Kurt P., President and Chief Executive Officer, U.S. Corporate and Federal Government Markets, LexisNexis	37
Smith, Derek, Chairman and Chief Executive Officer, ChoicePoint, Inc	44
ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD:	
Smith, Derek, Chairman and Chief Executive Officer, ChoicePoint, Inc, response for the record	94

PROTECTING CONSUMERS' DATA: POLICY ISSUES RAISED BY CHOICEPOINT

TUESDAY, MARCH 15, 2005

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

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2123 of the Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Bass, Pitts, Bono, Terry, Otter, Myrick, Murphy, Blackburn, Barton (ex officio), Schakowsky, Markey, Towns, Brown, Green, Strickland, DeGette, Gonzalez, and Baldwin.

Staff Present: David Cavicke, chief counsel; Chris Leahy, policy coordinator; Shannon Jacquot, majority counsel; Andy Black, deputy staff director; Brian McCullough, majority professional staff; Will Carty, majority professional staff; Bud Albright, staff director; Larry Neal, deputy staff director; Jon Tripp, deputy communications director; Kevin Schweers, communications director; Billy Harvard, legislative clerk; Julie Fields, special assistant to the policy coordinator; Consuela Washington, minority counsel; Jonathan Cordone, minority counsel; Edith Holleman, minority counsel; Voncille Hines, minority staff assistant; and Turney Hall, minority staff assistant.

Mr. STEARNS. Good morning, everybody. The subcommittee hearing today will come to order on Protecting Consumers' Data: Policy Issues Raised by ChoicePoint and identity theft.

Just like knowledge, information is power. In a world where information can be transmitted at the speed of light to anybody with the ability to access it, legitimately or fraudulently, there are a multitude of potential security issues that obviously can occur. The security of that information can be compromised within the sanctuary of the data base, along the pipeline of the network, and at the final destination, which in many cases, is a point of sale.

What is more worrying is that sensitive information and access to it involves very specific pieces about who we are, where we live, what we buy, how much money we make, what we drive, our criminal history, in fact, and so on. The growing business of commercial data collection and brokering has made products like packaged consumer information profiles tailored for specific requirements and clients, a major and important mode of business. These information products and their applications are becoming more sophisticated

and comprehensive, as advances in technology continue to improve the capability to collect, store, analyze, and package information, both personal and non-personal.

My colleagues, our focus today is directed at the apparent cracks in the comprehensive system of information sharing and brokering, including understanding how penetrable and vulnerable the data bases and network pipelines are, as well as assessing the accuracy and effectiveness of identity verification.

Now, the recent security breaches at two of the biggest and most sophisticated companies in the industry, ChoicePoint and LexisNexis, which are both represented here today, by their CEOs, serve to highlight the need for Congress and this committee to examine closely the effectiveness of the current regulatory regimes. This would include Federal law, like the Fair Credit Reporting Act, and State laws designated to protect and secure this highly sensitive information from the criminals working to breach these fortifications. These laws tend to operate independently in the marketplace, in addition to the State requirements. As a result, there is clearly a need to consider a comprehensive Federal consumer notification requirement, a uniform national standard, so that jurisdictional issues don't cause unnecessary problems for consumers victimized by this criminal activity. Any solution needs to ensure that consumers are notified as quickly as possible when these breaches occur. We owe that to every American. And additionally, recent events compel us to visit the fundamental privacy debate, as it relates to the power of the consumer to control the transmission of that data, ensure its accuracy, and be given notice when it is being used legitimately or compromised for nefarious purposes.

Now, as we all know, this hearing today is taking place against a backdrop of one of the most rapidly growing crimes in America, identity theft. As we will hear today, a recent Federal Trade Commission survey showed that almost 10 million people in the United States discovered that they were involved in some sort of identity theft. These numbers translate into losses of almost $50 billion for businesses and $5 billion for consumers. My colleagues, this is a huge and growing market for fraudsters, and according to some reports, for terrorist networks seeking to cash in in this lucrative crime.

The commercializing or monetarizing, as some may suggest, of consumer data has made protecting it far more complex and important, given its value in the wired marketplace. Today's cyberthieves employ high tech surveillance, in some case slip anonymously into secure data bases to complete the heist. More traditional criminals simply acquire official identification and business licenses fraudulently, then dupe the verification process used by the information company, and set up a shop to receive their first shipment of sensitive consumer financial data, personal data. These two case studies we have before us this morning, the high tech and mundane, are now in the headlines, and indicate the digital dike is starting to leak very sensitive information about ourselves to those who wish to do us harm. As we will learn, breaches can occur from inside companies as well. Data security firms, including the one joining us today are working on novel approaches

to secure data bases and network traffic before breaches destroy the financial soundness and privacy of thousands of Americans.

At the same time, my colleagues, the ability to access much of this personal information obviously facilitates legitimate commerce that benefits all of us today. Trusted third parties, including data brokers and financial institutions, facilitate important commercial and public functions through their ability to quickly and securely access vast amounts of consumer data. Their technology and products help us, for example, screen out risky job applicants from sensitive positions, obtain faster credit and more securely, pay less for our insurance products, and in a few dramatic cases, allow law enforcement to move quickly to find criminal suspects. Many people value these services and products, and may not even know about it.

Today's hearing is not an effort to demonize these legitimate practices and companies. But, my colleagues, it is, rather, an opportunity to understand the reasons behind the recent breaches, examine the legal regimes involved, and create a means by which consumers affected by a breach can be provided prompt and detailed notice, as well as an opportunity to verify and correct their personal information. The average consumers loves the convenience many of these systems provide, but obviously also want control over the details of his or her life, public or not.

The value of that information in today's digital marketplace, coupled with illicit motives, make its proper use harder to police. Accordingly, this committee must ensure that the commercial application of consumer information retains that careful balance between security, the protection of privacy, and liberty that every American holds so dear.

I would like to thank our panel, particularly the Chairwoman of the Federal Trade Commission, for being with us, and also, the CEOs of both ChoicePoint and LexisNexis, for their time and their willingness to come forward with their testimony.

With that, I recognize the Ranking Member, Ms. Schakowsky of Illinois.

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

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

Good Morning. Just like knowledge, information is power. And in a world where information can be transmitted at the speed of light to anyone with the ability to access it, legitimately or fraudulently, there are a multitude of potential security issues that can occur. The security of that information can be compromised within the sanctuary of the database, along the pipeline of the network, and at the final destination, which in many cases is the point of sale. What's more worrying is that sensitive information and access to it involves very specific pieces about who we are: where we live, what we buy, how much money we make, how we drive, our criminal history, and so on. The growing business of commercial data aggregation and brokering has made products like packaged consumer information profiles, tailored for specific requirements and clients, a major and important business. These information products and their applications are becoming more sophisticated and comprehensive as advances in technology continue to improve the capability to collect, store, analyze, and package information, both personal and non-personal. Our focus today is directed at the apparent cracks in the comprehensive system of information sharing and brokering, including understanding how penetrable and vulnerable the databases and network pipelines are, as well as assessing the accuracy and effectiveness of identity verification.

The recent security breaches at two of the biggest and most sophisticated companies in the industry, Choicepoint and LexisNexis, which are represented before us today by their chief executives, serve to highlight the need for Congress and this great Committee to examine closely the effectiveness of the current regulatory regimes. This would include federal law, like the Fair Credit Reporting Act, and state laws designed to protect and secure this highly sensitive information from the criminals working to breach those fortifications. These laws tend to operate independently in the marketplace, in addition to the state requirements. As a result, there is clearly a need to consider a comprehensive federal consumer notification requirement, a uniform national standard, so that jurisdictional issues don't cause unnecessary problems for consumers victimized by criminal activity. Any solution needs to ensure that consumers are notified as quickly as possible when breaches occur. We owe that to every American.

Additionally, recent events compel us to revisit the fundamental privacy debate as it relates to the power of the consumer to control the transmission of that data, ensure its accuracy, and be given notice when it's being used legitimately or compromised for nefarious purposes. As we all know, this hearing today is taking place against the backdrop of the most rapidly growing crime in America—identity theft. As we will hear today, a recent Federal Trade Commission survey showed that almost 10 million people in the United States discovered that they were involved in some sort of identity theft. These numbers translate into losses of almost $50 billion for businesses and $5 billion for consumers. This is a huge and growing market for fraudsters and, according to some reports, for terrorist networks seeking to cash in on this lucrative crime.

The commercializing or monetizing, as some may suggest, of consumer data has made protecting it far more complex and important given its value in the wired marketplace. Today's cyber-thieves employ high-tech surveillance and, in some cases, slip anonymously into secure databases to complete the heist. More traditional criminals simply acquire official identification and business licenses fraudulently, dupe the verification process used by the information company, and set up shop to receive their first shipment of sensitive consumer financial and personal data. These two case studies, the high-tech and mundane, are now in the headlines and indicate the digital dike is starting to leak very sensitive information about ourselves to those who wish to do us harm. As we will also learn, breaches can also occur from inside companies as well. Data security firms, including the one joining us today, are working on novel approaches to secure databases and network traffic before breaches destroy the financial soundness and privacy of thousands of Americans.

At the same time, the ability to access much of this personal information facilitates legitimate commerce that benefits all of us. Trusted third parties, including data brokers and financial institutions, facilitate important commercial and public functions through their ability to quickly and securely access vast amounts of consumer data. Their technology and products help us, for example, screen out risky job applicants from sensitive positions, obtain credit faster and more securely, pay less for our insurance products, and in a few dramatic cases, allow law enforcement to more quickly find criminal suspects. Many people value these services and products and may not even know it.

Today's hearing is not an effort to demonize those legitimate practices and companies, rather it is an opportunity to understand the reasons behind the recent breaches, examine the legal regimes involved, and create a means by which consumers affected by a breach can be provided prompt and detailed notice, as well as an opportunity to verify and correct their personal information. The average consumer loves the convenience many of these systems provide, but also wants control over the details of his life, public or not. The value of that information in today's digital marketplace coupled with illicit motives makes its proper use harder to police. Accordingly, this Committee must ensure that the commercial application of consumer information retain the careful balance between security, the protection of privacy, and liberty that every American holds so dear.

I would like to again graciously thank our distinguished panel of witnesses for joining us today. We look forward to your testimony. Thank you.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns, for holding this hearing today on the risks that consumers face, because the data brokers, like ChoicePoint, and problems that they have had. We were all shocked to hear that a few criminals were able to set up scams which jeopardized the personal and financial security of hundreds of thousands of people. We need to close the gaps in the

law that are putting consumers and their sensitive information at greater risk for privacy invasion, identity theft, and other crimes.

Stories of security breaches of data bases of personal and financial information have been all over the news in the past few weeks. Most notably, we have heard about ChoicePoint selling personal records of 145,000 people to sham businesses, and of con artists using real accounts and passwords to access 32,000 people's records in LexisNexis' Seisint data base.

My own State of Illinois has already ranked ninth in the Nation for identity theft cases, and the fact that 5,025 more residents are at greater risk because of the ChoicePoint's fumble, and 481 more, because of the LexisNexis' problem, I am even more troubled by these reports. Chairman Stearns, being that Florida is fifth in the Nation for ID theft, I know, and you just testified that you are quite aware that these breaches, what they can mean for consumers and our constituents.

While our witnesses will admit that some of the data accessed as a result of the breaches is sensitive personal information, including Social Security numbers and driver's license numbers, we are also going to hear disclaimers about how most of that information was from public records. Downplaying the security breaches does not provide me or many others with comfort. Although the information may be public, when those records are compiled and then linked to other information about consumers, the nature of those records is radically changed.

In fact, the power of aggregated information was one of the driving forces before the 1974 Privacy Act, which makes it illegal for government agencies to amass the kind of personal information that data brokers do today. Our Congressional predecessors knew that limits were needed to protect the people's privacy from government spying. What they did not realize was that Big Business would handle the dirty work for Big Brother, and that technology would make it possible to gather and store thousands of pieces of personal information which is available with just the click of a mouse.

Despite its power, profit, and reach, the burgeoning data brokerage industry is largely unregulated. The lack of regulation is seriously troubling for a number of reasons. First of all, data brokers sell their information to employers, insurance companies, debt collectors, government agencies, and in some cases, individuals. They see their role as being "risk mitigators" for their clients. However, the information they sell could cost people jobs, insurance, the right to vote, or even their lives, if the information is sold to a stalker or abusive spouse, for example.

The risk is shifted to defenseless and unaware people, at times crime victims. There are no guarantees that the information that data brokers are selling is accurate, and they have few, if any, obligations to consumers to correct it. Data brokers could blacklist people, and there is little victims can do about it. On top of that, as these recent breaches reveal, the very collection and sale of the information could mean that even more accurate information is added to—inaccurate, excuse me—that even more inaccurate information is added to consumers' records.

Already, 700 people who had their information bought by fraudsters from ChoicePoint have become victims to identify theft, and although ChoicePoint has promised to help them correct the problems they will incur, it will take these individuals on average 2 years or longer to clear their names. Even then, we have no guarantee that all their future records will reflect that, and who knows the costs they will incur along the way.

I find the lax security and regulation of data brokers especially disturbing because of the government reliance on them. One report put the number of government agencies using data brokers at around 7,000, from local police stations to the Department of Justice, with $67 million in contracts with ChoicePoint in 2004 alone. Hundreds of millions of dollars are flowing each year from the taxpayers' pockets and into the data brokers' banks. While I am troubled by the prospect that the government agencies may be violating the spirit of the 1974 Privacy Act, I am particularly concerned about the fact that they are turning to freewheeling contractors to get their information.

If we are going to be using taxpayer dollars to pay for these services, we need to make sure data brokers are accountable when it comes to the security and accuracy of the data they are compiling. People's very lives are at stake, and we do not need a Halliburton of the information industry, or another legal black hole through which contractors fall, and from which they profit.

Again, Chairman Stearns, I look forward to working with you and the other members of our committee, to do what we can to protect consumers. Thank you.

Mr. STEARNS. I thank the gentlelady. The chairman of the full committee, the distinguished gentleman from Texas, Mr. Barton, is recognized.

Chairman BARTON. Thank you, Mr. Chairman. Thank you for holding this hearing, and thank you, Commissioner, for being here. I would also like to recognize the former Chairman of the Science Committee, Bob Walker of Pennsylvania, is in the audience, and we appreciate him being here.

This is an important hearing. We are all very concerned about what has happened. Nobody takes this more seriously than I do, along with Congressman Markey of Massachusetts. We are original founders of the Privacy Caucus in the House, and in the Senate, the founders are Senator Chris Dodd of Connecticut, and Senator Shelby of Alabama. So I have not only a professional interest as Chairman of the Committee, but a personal interest as a privacy—co-chairman of the Privacy Caucus, with Mr. Markey here in the House.

It wasn't so long ago that your Social Security number was known to two people, yourself AND the Social Security Administration. I have stopped carrying my Social Security card. I have just memorized it, but if I forgot it, it wouldn't be very hard for me to get it. I could just almost touch base with any number of creditors and, I think, get it very easily. I didn't find out until I prepared for this hearing that your Social Security number is routinely given, along with other very sensitive information, a number of agencies—that data is collected by two of the companies that are before us today, that have had a problem, and that for almost any

purpose, it can be obtained rather easily. I think that is just wrong. I just think that is wrong. If I want to give my Social Security number to somebody, I will give it to them. I know if I go to the bank, and I want a loan, I am going to have to give them some information, and I will voluntarily disclose that in order to get the loan, or at least to be reviewed for the loan. But I don't see how it serves my purpose as an individual when my number and my information is routinely given without my permission. I just fundamentally think that is unfair. In the Internet age, it is just dangerous.

With the availability of information sharing and file sharing and all that over the Internet, it is just—it is frightening. Identify theft, consequently, is becoming one of the top issues in consumers' and voters' minds. My former wife had her Social Security number stolen and used for medical purposes at a hospital in Dallas, and only found out about it when the hospital tried to collect some emergency room charges. And since she was not in that hospital at any time for medical services, we were able to prove that it wasn't her. If somebody else had gotten her Social Security number, and tried to use it to get medical treatment in Dallas.

I understand that some of these groups that are here today provide a public service by collecting information and selling it, so that business groups can market legitimately their products, over the Internet and through the mail and by telephone. But I don't think that that is a guaranteed right, and I do believe that individuals have the right to know what is going on with their information. I think that after we hold this hearing, we are going to have to make a decision whether we need to set some national standards about what can be traded, when, and what you have to tell the individual that their own information is being used, and whether when, in this case, it is stolen, people should be notified of that. Currently, there is no Federal standard or Federal law that requires that.

Last year, according to the Federal Trade Commission, 10 million consumers were victims of identity theft. Ten million. That number is going up, and if you are one of those 10 million people, just getting your identity stolen is not the end of it. It takes years and years, sometimes, to clean up the damage of one inadvertent problem. We have a lot of members on this committee that are very interested in this issue. I have already mentioned Congressman Markey. Chairman Stearns has held a number of hearings on this. Congressman Shadegg, our whip on the committee, passed a Public Law, the Identity Theft and Assumption Deterrence Act of 1998, 7 years ago. So we are ready to go. We are going to hear our Chairman of the Federal Trade Commission. We are going to hear some of our private sector CEOs. Then we will hear some consumer advocates.

I don't know if this is the only hearing we are going to do on this. We may do another one. But some time this spring, we are going to sit down after we have listened and digested the testimony, and make a decision what legislative strategy, if any, we need to employ. But my guess is we are going to move forward with some Federal legislation on this issue, and with that, Mr. Chairman, I would yield back.

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

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

Thank you Mr. Chairman for holding this hearing today. It is no secret that privacy and information security are important to me. I co-founded the Congressional Privacy Caucus, and as Chairman of the Committee on Energy and Commerce, I have focused on Internet issues like the spyware legislation that passed out of the Committee by a vote of 43 to 0 just last week.

Not long ago, your Social Security number was between you and the government and nobody else. Nowadays, *everybody* seems to have your number. That knowledge is the key to your financial security. It opens a door for identity thieves to sneak into your life and steal both your money and your good name.

I just think this situation is fundamentally wrong any time. And in the Internet age, it's downright dangerous. Under current law, anyone has a near-perfect right to package your personal information and do almost anything they want with it. They can change it, share it, rent it or sell it. The constraints are so flimsy they're laughable.

Although I recognize the consumer benefits of an increased flow of information—such as easier and cheaper access to credit—I do believe that consumers should have some measure of control over their information. In particular, I believe that the businesses that benefit from the use of consumer information should bear greater responsibility for the security and integrity of that information. While specific industries and particular types of information are governed by Federal data security standards, Congress has not set comprehensive data security standards. It may be time we do so.

I believe we will need to consider whether there should be national standards for protecting consumers when their personal information is lost or wrongfully disclosed by a data broker. Consumers have no direct relationships with these data brokers. To data brokers, we are not customers—information about each of us is a product that is sold for many purposes, including marketing without our knowledge or consent.

I have been troubled by the press accounts that have revealed security breaches at companies in a range of industries from financial institutions, to data brokers, to retail outlets. Those breaches range from misplaced information to outright fraud by identity thieves. No matter the particular circumstances, these breaches demonstrate that American businesses must do more to outwit identity thieves, and this Committee must take the lead in developing appropriate safeguards for consumer information.

Identity theft is big business and the thieves are getting smarter and more resourceful. According to the Federal Trade Commission, approximately 10 million consumers were victims of identity theft in 2003. It is estimated that in 2003, identity theft victims spent 297 million hours trying to clear up the problems and their reputations.

Even after unauthorized credit cards are closed and charges are settled, it can take years for an innocent consumer to repair a credit report. All the while, home ownership and other personal goals innate to the American Dream could be out of reach. Data brokers do not bear direct responsibility, but we have to ask: What are these companies doing to cure the epidemic of identity theft?

This Committee has a deep bench of experts in the areas of identity theft and privacy. Chairman Stearns has held numerous hearings parsing through important issues surrounding information privacy and security. Representative Shadegg was the author of an important public law, the Identity Theft and Assumption Deterrence Act of 1998. That Act has provided significant tools for enforcement against identity theft. It also directed the Federal Trade Commission to set up an identity theft consumer resource center. That center has been a success as it has gathered important information regarding identity theft, acted as a central repository for complaints, and provided important consumer education. I am pleased Chairman Majoras is here to testify today as she brings much expertise in this area. I am eager to hear her proposals for better and more comprehensive Federal data security standards.

I would also like to welcome the other witnesses today and I thank them in advance for their testimony. We have a number of witnesses with busy schedules and we appreciate their cooperation and assistance in working through these challenging policy questions. Thank you and I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman. Ms. Baldwin, from Wisconsin. I think. He was the first one here. She was the first, actually. Mr.——

Ms. BALDWIN. Representative Markey was here before me. I——

Mr. STEARNS. Oh, okay.

Ms. BALDWIN. He greeted me as I walked in the door.

Mr. STEARNS. All right. Good. I am glad you corrected. The gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. I thank the chairman very much. And I would like to reiterate what the chairman of the full committee just said, which is that this is an issue which knows no political boundaries. Chairman Barton and I co-founded the Privacy Caucus, 7 or 8 years ago, because there is a point on privacy issues where the libertarian right and the liberal left agree wholeheartedly, and that is that the privacy of individuals should be inviolate.

Now, we find that there is a pragmatic middle that argues that it interferes with the ability of businesses to make money off of the privacy of individuals, but whether you are a Democrat or a Republican, regardless of your age, it all polls out the same way. Eighty percent to 90 percent of all Americans want stronger privacy protections. And Chairman Barton and Chairman Stearns and I, Democrats and Republicans, Jan Schakowsky, we all agree on this issue. Americans take privacy seriously. We guard our credit cards by carefully returning them to our wallets. We keep our mortgage records and Social Security cards and personal documents locked up.

How would consumers feel if they discovered that while they take extra precautions to guard their personal information, their names, Social Security numbers, tax records, credit histories, and employment records were piled high into wheelbarrows and baskets, and sold to the highest bidder, in a bustling marketplace that is as frenetic and unregulated as the streets of Bombay? Right here, get your Social Security numbers, medical records, employment history, cheaper by the dozen. Come, purchase them, the records of all Americans. How would we all feel that our Social Security number was in some identity vendor's suitcase of wares? How would we feel? We would feel violated. That is exactly how two of my constituents, Kei and Karen Kishimoto felt this week, when they wrote me about a letter they received from ChoicePoint, stating that they were among the 145,000 victims whose Social Security numbers and other sensitive and personal data were compromised by ChoicePoint.

"We are furious," they wrote, "that ChoicePoint has irresponsibly allowed this to happen. We take every precaution within our power to minimize our risk of becoming victims of identity theft." These are just two of 145,000 victims. They had no choice about this, and that is the point. They all feel violated, each and every one of them. And so as this scandal grows, we must legislate. I have introduced one piece of legislation with Senator Bill Nelson from Florida, which would require the FTC to put tough new safeguards in place, that all of these information brokers will have to abide by, and I have a second bill, that Senator Feinstein, in the Senate, has the counterpart to, that I have introduced for several years, that will make it a crime for a person to sell someone's Social Security numbers. I think we have reached a point where all of America, through ChoicePoint, has begun to understand how vulnerable each and every one of their families has become.

I thank you, Mr. Chairman, for holding this very important hearing.

Mr. STEARNS. I thank the gentleman. Mr. Terry is—if Terry is not here, then Mr. Murphy.

Mr. MURPHY. Thank you, Mr. Chairman. Thank you for holding this very important meeting on a topic that is both timely and pertinent in today's world.

Today, the Federal Trade Commission Chairman will remind us that this committee, that in 2003, the FTC estimated almost 10 million Americans were the victims of identity theft. In the last 5 years alone, the FTC estimates that 27 million Americans have been victims, costing consumers more than $5 billion. Nary a week goes by that I do not see a story on the nightly news about the dire effects consumers suffer when they fall victims to identify theft.

The term "identity theft" has unfortunately become commonplace in the American lexicon. Yet, it is important to take a second to consider the term and the crime, and remember that it is, in fact, a crime as heinous as burglary or extortion. The perpetrators of these crimes are the bane of e-commerce, and must be hunted down, prosecuted, and imprisoned for a long while.

Too often we hear of schemes involving numerous consumer victims, and we focus on the companies that were also victimized, instead of placing the blame squarely on the shoulders of the terrorists who perpetrate these crimes. Recent events have brought this topic into the limelight. ChoicePoint and LexisNexis were both victims of malicious and fraudulent crimes. ChoicePoint was deceived into selling aggregated consumer data to criminals, who may or may not have used it to defraud upwards of 150,000 consumers. According to early estimates, data from almost 2,000 Pennsylvanians were placed in jeopardy, and similarly, a LexisNexis data base was subject to criminal hacking, which resulted in thousands of customers being placed at risk for financial fraud being committed against them.

I am alarmed at the amount of personal information that most of think to be private is sold and traded every day without the knowledge of the actual person. It is important for Congress and especially this committee to be vigilant in monitoring the personal data commodity markets, because an infinitesimal number of consumers actually are aware of how much their information is publicly available for companies to purchase without giving you a dime. It is equally important not to fear-monger on this topic. The ability of data aggregators to provide accurate information about individuals is vital to our credit-based economy, and has become essential to law enforcement, and a vital component in our homeland security network.

Every one of us submits to providing the detailed information almost every time we enter into contract with a vendor, whether it is for a credit card or even a newspaper subscription. Some companies refuse to sell consumer—customer information to data aggregators. If companies wish not to have their data traded or disseminated, then they should seek out such companies. However, it is important to emphasize that we are not holding this hearing to take gratuitous potshots at an industry that is vital. We are here this morning to figure out what the industry and Federal Govern-

ment are doing to ensure consumer data does not fall prey to criminals who will use it to defraud.

I am eager to hear from the witnesses, and stand ready to take legislative actions to further protect consumers, and more harshly punish the pirates that commit these crimes.

Thank you.

Mr. STEARNS. I thank my colleague. The gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman.

Over the past quarter century, we have all witnessed the revolution in information technology, and with access to the right data bases, a touch of the button, vast amounts of information about a person can be immediately accessed, their date of birth, Social Security number, credit rating, debt, loans, insurance claims, magazine subscriptions, and even DNA information. Much of this information is relatively easily accessible to companies for a variety of legitimate purposes, but such broad compilations raise significant concerns that have been insufficiently considered by this Congress, and more generally, by the American people.

First, how do we ensure that the data is not misused? The potential here for fraud and abuse is significant, and as we know from the Federal Trade Commission, identity theft accounted for 39 percent of consumer fraud complaints in 2004. Unfortunately, this problem is far greater than just ChoicePoint.

Second, how do we ensure that the data is accurate? The everyday lives of Americans are affected by business decisions based on personal information dossiers that are compiled without their knowledge or input. A person has no easy way to review that data, or determine that the information is accurate or, perhaps, inaccurate, misleading, perhaps incomplete. And I realize, Mr. Chairman, that that second question is beyond the scope of today's hearing, but I do hope that the subcommittee will also focus on this question in the near future.

I am concerned that there is an inadequate and a sort of patchwork of laws and regulations that cover and govern the collection, compilation, distribution, and use of aggregated personal and financial information. Today, I hope to hear from our witnesses, as they articulate ways in which we can protect consumers from identity theft and other misuses of their data.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady. The gentlelady from Wisconsin—from California, Ms. Bono. Waive, the gentlelady waives. Mr. Deal. Waive. Mr. Pitts. Pass. Mr. Otter. Ms. Blackburn. Waive, okay. Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman.

Instead of data brokers, it is probably better to think of companies like ChoicePoint as data banks. Like financial banks, they hold something valuable, and by choosing to profit from what they store, they must accept the responsibility to protect it from those who misuse it. Imagine that the bank down the street has been robbed repeatedly. The vault lock is pretty old, the night watchman's vision isn't what it used to be, and they have no alarm system. The crooks know the bank is an easy mark, so the depositors keep taking it on the chin. Would we respond, would we even con-

sider responding only with tougher bank robber penalties in mandatory robbery disclosure? Of course not. We would make sure that the bank got a state-of-the-art lock, perhaps Lasik surgery for the guard, and an alarm system designed maybe for a nuclear missile silo.

We have to consider a similar approach here. We ought to give the FTC clear authority to set and enforce tough rules for data protection. We ought to make all these rules seamless, so the bad guys can't sneak in through the cracks, and we ought to put the—use the government's purchasing power to promote best practices that take security beyond the bare minimum. If the Federal Government fails to respond that way here, with a comprehensive approach, we are as negligent as the data brokers who allowed these violations to occur in the first place.

The economic impact of the crimes resulting from ChoicePoint's negligence may reach the tens of millions of dollars, but in a broader context, the stakes are much higher. ChoicePoint, this same company, is famous, or should I say infamous, for a mistake with the voter files in Florida during the 2000 Presidential election. Its error, coupled with the errors of public officials, disenfranchised thousands of African-American voters, and may have decided the Florida elections and the Presidential elections. But ChoicePoint, with all of its political connections to the highest levels of the government in this country, was not the only party at fault. The politician who chooses a contractor to perform a basic government function, like administering elections, is just asking for trouble, and the costs of contracting out are not measured only in terms of dollars.

The lesson here, and I urge my colleagues to remember all of that the next time someone suggests a privatization plan, a privatization of any function that has been performed effectively and efficiently, and honorably and honestly, by our government. And I urge this subcommittee to act thoughtfully, but quickly, on legislation to reform the data brokerage industry.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Mr. Green. No, let's see. Coming back over here. Okay. Now, Mr. Green. Yeah. The gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I would like to have my full statement in the record, and I won't use all my time.

Mr. STEARNS. By unanimous consent, so ordered.

[The prepared statement of Hon. Gene Green follows:]

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

I'd like to thank Chairman Stearns and Ranking Member Schakowsky for taking the lead on this issue and holding this important hearing. I'd also like to welcome Chairwoman Majoras for being here today. Your cooperation and willingness to share your knowledge and experience with this committee is imperative to our success in combating data and identity theft.

Also, Mr. Smith and Sanford are to be commended for being here as the leaders of their companies to share with us how their business works, what's wrong with the current system and how we might be able to fix it.

Identity theft is the number one crime in the United States. The FTC estimates about $48 billion is lost each year to business due to this crime, and $5 billion to consumers. We have held an Identity Theft Workshops for our constituents so they know what they can do to lower the chance that someone can access their information.

These workshops only work when credit reporting agencies, financial institutions and data brokers do their job to make sure information doesn't fall into the wrong hands.

Now more than ever, we've "become a number": Most often, than number is our Social Security Number. Every financial institution uses that number to verify that you are who you say you are.

Most of the time, this system works. However, when the information has been stolen and others have been using your name to get credit, make purchases, or start phony businesses, the results can be tragic. Without good credit, you can't buy a home, you may be turned down for a job and it can take months even years to repair the damage that's been done.

Our current systems of laws addressing this problem are piecemeal. We have the Fair Credit Reporting Act to address Credit Reporting Agencies. The Federal Trade Commission Act addresses unfair and deceptive trade practices. There is a separate law for Drivers License data, Gramm-Leach—bliley addresses Financial Institutions and of course, there's HIPPA, which protects the security of our medical records.

Today, there is no encompassing law that addresses this problem on the federal level. I believe this is one of the problems. While I support crafting legislation specifically to address the unique uses of information, we have not sent a message to Americans that this is something we are going to be tough on regardless of what type of information is stolen or misused.

In the case of ChoicePoint, information was sold to a faulty business and approximately 145,000 people are at risk of having their information used without their knowledge. Hundreds are reported to have already been affected in California.

Choice Point brokers information for a variety of purposes and does so through some of their subsidiaries such as Database Technologies (DBT). DBT was contracted with the State of Florida in 2001 and was responsible for the removal of almost ten thousand minorities and eligible voters from the rolls in Florida which threw our country into uncertainty for several days while we determined who was elected President of the United States.

In addition, Choice Point DNA data was used to help identify many of the victims on September 11. The scope of the information out there is immense and the responsibility that comes with collecting and selling this information is just as large.

We are here today to begin a dialogue with industry, the FTC and our colleagues to see what we can do to make our information as secure as possible. Billions of dollars can be made by using this information illegally. There will always be those who want to obtain this information for illegal purposes. Our purpose is to improve the safeguards to the consumer.

As we will hear today, this issue is complex. However, what is clear is that something needs to be done to improve the security of our identities. I believe requiring notification of individuals affected by a security breech is where we should start.

I look forward to working with all of you on this important issue.

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

Mr. GREEN. But I just wanted to make three points.

One of them, I want to welcome our FTC Chairman here today, and identity theft is such a major issue, and when we heard about what happened with ChoicePoint, it was frustrating, because ChoicePoint may have provided the data for 140,000 people, and I know they have a great deal of data. The bad part is, is that they also struck some voters off the rolls in Florida in 2001, but the good point is they were helping, they actually helped victims of 9/11 to identify the folks.

The problem I have is that I know, under Federal law now, we are allowed, our constituents and ourselves are allowed copies of—annually, of our credit reports from the three major agencies. But I have a copy of an MSNBC report about a lady, Donna Pierce, who received her ClearPoint, or—sorry, ChoicePoint document, and yet, it wasn't supposed to be in our hands. Does not—does Federal law not allow me to ask ChoicePoint, I want to see what you have on me?

If it is not, Mr. Chairman, we need to make sure that changes, because if it is my information, I ought to have access to it and correct it, just like we have now for our three major credit agencies.

With that, Mr. Chairman, I will put my full statement in the record. Thank you.

Mr. STEARNS. I thank the gentleman. Mr. Otter.

Mr. OTTER. Thank you, Mr. Chairman. I have a full statement that I would like to submit for the record.

But just a couple of points that I would like to make that, so far, no member on either side of the aisle has made. And that is, in my belief, that your information is actually your private property. And maybe it is our general disregard in this country, any more, for private property, copyright, patent, creative genius, or what have you. That is your private property, and so long as you are engaged in peaceful use of that private property, then it is the government's job to protect that.

Yet, I also note, from the chairman, from the full committee chairman, who was just, I asked him, in his recollection, is there any law or any punishment for even a government bureaucrat, saying the IRS, or saying some other information gathering, Medicaid, Medicare, entity of government, is there a penalty for them giving out private information? And so far as we have been able to ascertain, there is none.

So Mr. Chairman, this is far and reaching, and I think if we just look at the private sector and the private sector only, and forget about our privacy, and forget about our personal rights to peaceful use of our privacy, we are making a big mistake. I do appreciate your having this hearing, and allowing a broad perspective research and development of this issue.

Thank you, Mr. Chairman.

[The prepared statement of Hon. C.L. "Butch" Otter follows:]

PREPARED STATEMENT OF HON. C.L. "BUTCH" OTTER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF IDAHO

I would like to thank the chairman for holding this hearing. I think it is an extremely important issue and believe we have a real opportunity to assist businesses and their customers in providing a safe electronic marketplace.

In recent years there has been an increased awareness of identity theft, yet we still hear relatively little about the losses associated with these thefts.

While there will always be those who are dishonest and seek to scam the system, we must be more diligent in protecting our electronic assets and information. A system of shields employed to provide protections is certainly in the best interest of both consumers and companies that rely on the Internet to conduct business.

I am very interested in hearing from the witnesses today on what role they believe the government has in safeguarding consumers and companies that rely on the Internet and electronic transactions to conduct business.

Mr. Chairman, I thank you again for the opportunity to examine this issue and I look forward to hearing from the witnesses.

Mr. STEARNS. I thank the gentleman from Idaho. Mr. Gonzalez, the gentleman from Texas.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. I will be brief. But I was on Financial Services when the Fair Credit Reporting Act and reauthorization and what we were thinking of doing came up, and I was there when the Gramm-Leach-Bliley Act came up, and we voted it out.

And the big question, then, was recognizing the economic realities of how people do business, and the need to, of course, acquire

and store, exchange and share information, and it was quite a debate. We finally came up and recognized realities. But what we are faced with today is something that everybody feared, and that is okay, what about the safekeeping and the proper sharing with the proper individuals that are entitled to the information? We assumed, of course, that there would be some mischief out there, but maybe never to the scale that we are experiencing today, with some of the stories that are out there in the press, and what we are dealing with this morning.

The question then comes down to, because you have heard how strongly members on both sides of the aisle feel about the nature of this information. If you can't protect it, if you cannot secure it, should it be out there at all? And if we are not going to have that kind of information collection and sharing, how does it, then, impact the day to day businesses of what we do in this country? And so I think we have to really keep the two issues, and see if we can still, you know, come up with some solutions to make sure that we don't impact the bigger and greater picture out there, of the necessity for responsible collection and sharing of information.

I yield back.

Mr. STEARNS. The gentleman yields back. The gentlelady from Colorado.

Ms. DEGETTE. Thank you. Mr. Chairman, I would ask unanimous consent to put my full statement in the record.

Mr. STEARNS. By unanimous consent.

Ms. DEGETTE. Let me just make a couple of points.

There is a real human face on this problem. Thirty-two thousand people, people, our constituents, were affected by the incidence at LexisNexis, and credit card numbers were stolen from customers of over 100 stores at a popular retailer. One hundred fourty-five thousand people were affected by the ChoicePoint security lapse, and of course, 1.2 million Federal workers now know that the Bank of America has lost computer tapes that contained confidential financial data.

And what all of this shows together is that the information broker business needs a closer look. These companies are dealing in the business of people's most confidential information, their Social Security numbers, their credit card data, their driver's license records, and their other personal information, and this is information that belongs to millions and millions of people.

If these companies are vulnerable to hacking and other fraudulent practices, which obviously they are, then we have no choice but to draw the conclusion that the privacy and overall security of our citizens is at risk, and so I am looking forward to hearing more from the FTC about the recent study that was released showing that in a 1-year period, over 10 million people in this country had their personal information stolen and used in a fraudulent manner, and I am hoping that there is some idea as to the new tools that we can use to deal with this growing problem.

Society pays a great price, frankly, the citizen's personal information is available to criminals. The economy suffers because of business losses, and to individuals who are victims of identity theft, it can be utterly devastating, and it takes huge numbers of hours for people to try to deal with this. And so, Mr. Chairman, I, like every-

one else, am glad that you had this hearing to decide what tools we have in place to combat this problem, but more importantly, I am looking forward to, as a committee, determining what more may need to be done to protect this very sensitive data.

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

Mr. STEARNS. I thank the gentlelady. The gentleman, Mr. Towns, from New York.

Mr. TOWNS. Thank you very much, Mr. Chairman, for holding this hearing.

The recent high profile cases of consumers' personal data being unwittingly sold or stolen has brought this issue to the forefront. The American public is looking for answers to how data brokers, such as ChoicePoint, could make such a glaring error. I am hopeful today's hearing will begin the important process of examining our current laws, and help our committee determine what we can do to strengthen those laws, or improve enforcement of our existing statutes.

I have had a longstanding interest in protecting consumers' privacy. I first began advocating for safeguarding medical records when I found my own medical records in a public trash bin, and of course, the hospital had closed, and they threw the records out, and the records were just there for anybody to grab or to see, and in response, I introduced a bill protecting the privacy rights of insurance claimants, which became part of HIPAA.

Since last Congress, I have been working with my colleague, Congresswoman Mary Bono, to protect consumer privacy on the Internet from spyware. Our committee passed this bill last week, and I am hopeful that we can send it to the President's desk before the end of this year. But perhaps most frightening is the ability of these large companies to aggregate data, so that almost anything can be found out about you by a wide range of people.

On one hand, ChoicePoint should be commended for using its data to help clear wrongly convicted felons, as part of the Innocence Project. However, on the other hand, its data was mistakenly used to wrongly disenfranchise thousands of African-American voters in the 2000 election.

I look forward to hearing from our witnesses today, Mr. Chairman. I think this is a very important hearing, and I think that what we do here will determine the lives of many, in terms of what they will go through in years to come. So I look forward to hearing from the witnesses.

Mr. STEARNS. I thank the gentleman. I think we are ready. Mr. Terry, did you have—I will—glad to consider. All right.

With that, we will have our first panel. Mr. Strickland. I am sorry. Did you have an opening statement?

Mr. STRICKLAND. No, thank you, Mr. Chairman.

Mr. STEARNS. Okay. I thank the gentleman. With that, I think the opening statements are complete.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this timely markup.

I would like to thank the three panels of witnesses who have agreed to join us today. The subcommittee has compiled a very respectable list of witnesses who will

be able to offer us several distinct looks at the role of data collection agencies, how these corporations operate, and the federal laws governing these information services. The brokerage of personal information is a complex issue, and I look forward to benefitting from the testimony offered today.

Throughout my tenure on this subcommittee, we have continuously addressed issues relating to privacy protection and the ability of third parties to access and distribute personally identifiable information. As we will hear today, there are most certainly valid and appropriate roles for personal data collection. You can't argue with the role data collection agencies play in prosecuting criminals and monitoring national security threats. However, with the rapid advance of technology, the definition of "theft" has been dramatically altered. For every genuine and useful role of data collection, there seems to be a corresponding opportunity to use this information in a criminal nature.

Internet technology has opened the doors to business and consumer opportunities and increased educational access to millions, and this increased access is particularly important to the rural areas of Wyoming I represent. However, this increasing reliance on web-based technologies has opened the door for new crimes. As I said, many of the people in Wyoming enjoy the benefits of the internet, but these same folks still hold fast to the values of honesty and integrity. These principles should not have to be compromised to enjoy the benefits of internet technology.

It is my hope that today's hearing will open a dialogue that will demonstrate if Congress is doing enough to protect the common citizen from blatant crime and deception posed by identity theft. I also hope to hear suggestions regarding what consumers can immediately do to protect themselves from identity theft.

Again, I thank the Chairman, and I yield back the balance of my time.

Mr. STEARNS. We welcome the Chairwoman of the Federal Trade Commission, Deborah Platt Majoras, for her opening statement, and I am very glad to have her. And I had an opportunity to meet with her, and we were very impressed, and worked in—close together with Tim Muris, your predecessor, and we hope we can do the same with you, and we have followed your testimony on the Senate Banking Committee, so we hope to hear from you again, and with that, welcome.

STATEMENT OF DEBORAH PLATT MAJORAS, CHAIRMAN, FEDERAL TRADE COMMISSION

Ms. MAJORAS. Thank you very much, Mr. Chairman, members of the committee. I am Deborah Majoras, Chairman of the Federal Trade Commission. I am grateful for the opportunity to testify about identity theft, security of consumer information, and in particular, the collection of that information by data brokers.

Although the views expressed in the written testimony represent the views of the Commission, my oral presentation and responses to your questions are my own, and do not necessarily represent the views of the Commission or any other individual Commissioner.

Recent revelations about security breaches that have resulted in disclosure of sensitive personal information about thousands of consumers have put a spotlight on the practices of data brokers like ChoicePoint that collect and sell this information. The data broker industry includes many types of businesses, providing a variety of services to an array of commercial and governmental entities. Information sold by data brokers is used for many purposes, from marketing to assisting in law enforcement.

Despite the potential benefits of these information services, the data broker industry is the subject of both privacy and information security concerns. As recent events demonstrate, if the sensitive information they collect gets into the wrong hands, it can cause serious harm to consumers, including identity theft.

As every member here has acknowledged today, identity theft is a pernicious problem. As has also been acknowledged several times today, our recent survey estimated that as many as 10 million consumers discovered that they were victims of some form of identity theft in the 12 months preceding this survey. That is 4.5 percent of our adult population, and it represented an estimated nearly $5 billion in losses to consumers, and $48 billion in losses in business. We must look at ways to reduce identity theft, which has shaken consumer confidence to the core.

One means of reducing identity theft is to ensure that sensitive, nonpublic information that is collected by data brokers is maintained securely. There is no single Federal law governing the practices of data brokers. There are, however, statutes and regulations that address the security of the information they maintain, depending on how the information was collected, and how it is used. The Fair Credit Reporting Act, for example, makes it illegal to disseminate consumer report information, like credit reports, to someone who does not have a permissible purpose, that is, a legitimate business purpose for using that information. Thus, data brokers are only subject to FCRA's requirements to the extent that they provide consumer reports as that is defined in the statute.

Similarly, the Gramm-Leach-Bliley Act, which the Commission also enforces, imposes restrictions on the extent to which financial institutions may disclose consumer information related to financial products and services. Under GLB, the Commission issued its Safeguards Rule, which imposes security requirements on a broadly defined group of financial institutions that hold customer information, and the Commission recently brought two cases in which we alleged the companies had not taken reasonable precautions to safeguard consumer information.

And finally, Section 5 of the FTC Act prohibits unfair or deceptive practices by a broad spectrum of businesses, including those involved in the collection or use of consumer information. Using this authority, the Commission has brought several actions against companies that made false promises about how they would use or secure sensitive information, and these cases make clear that an actual breach of security is not necessary for an enforcement actions under Section 5, if the Commission determines that the company's security procedures were not reasonable in light of the sensitivity of the information being maintained. Evidence of a breach, of course, though, may indicate that the company's procedures were not adequate.

Now, it is important to remember that there is no such thing as perfect security, and breaches can occur, even for companies that have taken reasonable precautions. The Commission, consistent with the role that Congress gave us in 1998, has worked hard to educate consumers and business about the risks of identity theft, and to assist victims and law enforcement officials. The Commission maintains a website and a toll-free hotline, staffed with trained counselors, who advise victims on how to reclaim their identities.

We receive roughly 15,000 to 20,000 contacts per week on the hotline, or through our website, or mail from victims, and from consumers who want to avoid becoming victims. The Commission also

facilitates cooperation, information sharing, and training among Federal, State, and local law enforcement authorities fighting this crime.

Although data brokers are currently subject to a patchwork of laws, depending on the nature of their operations, recent events clearly raise the issue of whether these laws are sufficient to ensure the security of this information. I believe that there may be additional measures that would benefit consumers. Although a variety of proposals have been put forward, and all should be considered, the most immediate need is to address the risks to the security of the information.

Extending the Federal Trade Commission's Safeguards Rule to sensitive personal information collected by data brokers is one sensible step that could be taken. It also may be appropriate to consider a workable Federal requirement for notice to consumers when there has been a security breach that raises a significant risk of harm to consumers.

Mr. Chairman, members of the committee, the FTC shares your concern for the safety for the security of consumer information. We have been working hard on this issue, and we will continue to take all steps within our authority to protect consumers.

I thank you for the opportunity to discuss this vitally important subject, and I would be happy to respond to your questions.

[The prepared statement of Deborah Platt Majoras follows:]

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

I. INTRODUCTION

Mr. Chairman and members of the Subcommittee, I am Deborah Platt Majoras, Chairman of the Federal Trade Commission.[1] I appreciate the opportunity to appear before you today to discuss the laws currently applicable to resellers of consumer information, commonly known as "data brokers."

Data brokers provide information services to a wide variety of business and government entities. The information they provide may help credit card companies detect fraudulent transactions or assist law enforcement agencies in locating potential witnesses. Despite these benefits, however, there are concerns about the aggregation of sensitive consumer information and whether this information is protected adequately from misuse and unauthorized disclosure. In particular, recent security breaches have raised questions about whether sensitive consumer information collected by data brokers may be falling into the wrong hands, leading to increased identity theft and other frauds. In this testimony, I will briefly describe what types of information data brokers collect, how the information is used, and some of the current federal laws that may apply to these entities, depending on the nature of the information they possess.

All of this discussion takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. A 2003 FTC survey showed that over a one-year period nearly 10 million people—or 4.6 percent of the adult population—had discovered that they were victims of some form of identity theft.[2] As described in this testimony, the FTC has a substantial ongoing program both to assist the victims of identity theft and to collect data to assist criminal law enforcement agencies in prosecuting the perpetrators of identity theft.

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any individual Commissioner.

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

II. THE COLLECTION AND USE OF CONSUMER INFORMATION[3]

The information industry is large and complex and includes companies of all sizes. Some collect information from original sources, 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 small companies or the general public.

A. Sources of Consumer Information

Data brokers obtain their information from a wide variety of sources and provide it for many different purposes. The amount and scope of information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. Some data brokers, such as consumer reporting agencies, store collected information in a database and allow access to various customers. Some data brokers may collect information for one-time use by a single customer. For example, a data broker may collect information for an employee background check and provide that information to one employer.

There are three broad categories of information that data brokers collect and sell: public record information, publicly-available information, and non-public information.

1. Public Record Information

Public records are a primary source of information about consumers. This information is obtained from public entities and includes birth and death records, property records, tax lien records, voter registrations, licensing records, and court records (including criminal records, bankruptcy filings, civil case files, and judgments). Although these records generally are available to anyone directly from the public agency where they are on file, data brokers, often through a network of subcontractors, are able to collect and organize large amounts of this information, providing access to their customers on a regional or national basis. The nature and amount of personal information on these records varies with the type of records and agency that created them.[4]

2. Publicly-Available Information

A second type of information collected is information that is not from public records but is publicly available. This information is available from telephone directories, print publications, Internet sites, and other sources accessible to the general public. As is true with public record information, the ability of data brokers to amass a large volume of publicly-available information allows their customers to obtain information from an otherwise disparate array of sources.

3. Non-Public Information

Data brokers may also obtain personal information that is not generally available to members of the public. Types of non-public information include:

- Identifying or contact information submitted to businesses by consumers to obtain products or services (such as name, address, phone number, email address, and Social Security number);
- Information about the transactions consumers conduct with businesses (such as credit card numbers, products purchased, magazine subscriptions, travel records, types of accounts, claims filed, or fraudulent transactions);
- Information from applications submitted by consumers to obtain credit, employment, insurance, or other services (such as information about employment history or assets); and

---

[3] For more information on how consumer data is collected, distributed, and used, see generally General Accounting Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this Information* (GAO-04-11) (2004); General Accounting Office, *SSNs Are Widely Used by Government and Could be Better Protected, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO-02-691T) (statement of Barbara D. Bovbjerg, April 29, 2002); 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 has also held two workshops on the collection and use of consumer information. An agenda, participant biographies, and transcript of "Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information," held on June 18, 2003, is available at http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html. Materials related to "The Information Marketplace: Merging and Exchanging Consumer Data," held on March 13, 2001, are available at http://www.ftc.gov/bcp/workshops/infomktplace/index.html.

[4] Specific state or federal laws may govern the use of certain types of public records. For example, the federal Driver's Privacy Protection Act, discussed *infra,* places restrictions on the disclosure of motor vehicle information.

- Information submitted by consumers for contests, website registrations, warranty registrations, and the like.

B. Uses of Consumer Information

Business, government, and non-profit entities use information provided by data brokers for a wide variety of purposes. For example, the commercial or non-profit sectors may use the information to:

- Authenticate potential customers and to prevent fraud by ensuring that the customer is who he or she purports to be;
- Evaluate the risk of providing services to a particular consumer, for example to decide whether to extend credit, insurance, rental, or leasing services and on what terms;
- Ensure compliance with government regulations, such as customer verification requirements under anti-money laundering statutes;
- Perform background checks on prospective employees;
- Locate persons for a variety of reasons, including to collect child support or other debts; to find estate beneficiaries or holders of dormant accounts; to find potential organ donors; to find potential contributors; or in connection with private legal actions, such as to locate potential witnesses or defendants;
- Conduct marketing and market research; and
- Conduct academic research.

Government may use information collected by data brokers for:

- General law enforcement, including to investigate targets and locate witnesses;
- Homeland security, including to detect and track individuals with links to terrorist groups; and
- Public health and safety activities, such as locating people who may have been exposed to a certain virus or other pathogen.

These are just some examples of how these entities use information collected by data brokers.

It is important to understand that the business of data brokers could cover a wide spectrum of activities, everything from telephone directory information services, to fraud data bases, to sophisticated data aggregations.

III. LAWS CURRENTLY APPLICABLE TO DATA BROKERS

There is no single federal law that governs all uses or disclosures of consumer information. Rather, specific statutes and regulations may restrict disclosure of consumer information in certain contexts and require entities that maintain this information to take reasonable steps to ensure the security and integrity of that data. The FTC's efforts in this area have been based on three statutes: the Fair Credit Reporting Act ("FCRA"),[5] Title V of the Gramm-Leach-Bliley Act ("GLBA"),[6] and Section 5 of the Federal Trade Commission Act ("FTC Act").[7] Although the FCRA is one of the oldest private sector data protection laws, it was significantly expanded in 1996 and in the last Congress. The Commission is engaged in a number of rulemakings to implement the new provisions of the FCRA, many of which are directly targeted to the problem of ID Theft. The GLBA is a relatively recent law, and its implementing rule on consumer information privacy became effective in 2001. Other laws, such as the Driver's Privacy Protection Act[8] and the Health Insurance Portability and Accountability Act[9] also restrict the disclosure of certain types of information, but are not enforced by the Commission. Although these laws all relate in some way to the privacy and security of consumer information, they vary in scope, focus, and remedies. Determining which—if any—of these laws apply to a given data broker requires an examination of the source and use of the information at issue.

A. The Fair Credit Reporting Act

Although much of the FCRA focuses on maintaining the accuracy and efficiency of the credit reporting system, it also plays a role in ensuring consumer privacy.[10] The FCRA primarily prohibits the distribution of "consumer reports" by "consumer reporting agencies" ("CRAs") except for specified "permissible purposes," and re-

[5] 15 U.S.C. §§1681-1681u, as amended.
[6] 15 U.S.C. §§6801-09.
[7] 15 U.S.C. § 45(a).
[8] 18 U.S.C. §§2721-25.
[9] 42 U.S.C. §§1320d *et seq.*
[10] "[A] major purpose of the Act is the privacy of a consumer's credit-related data." *Trans Union Corp. v. FTC,* 81 F.3d 228, 234 (D.C. Cir. 1996).

quires CRAs to employ procedures to ensure that they provide consumer reports to recipients only for such purposes.

1. Overview

In common parlance, the FCRA applies to consumer data that is gathered and sold to businesses in order to make decisions about consumers. In statutory terms, it applies to "consumer report" information,[11] provided by a CRA,[12] limiting such provision for a "permissible purpose."[13] Although the most common example of a "consumer report" is a credit report and the most common CRA is a credit bureau, the scope of the FCRA is much broader. For example, there exist many CRAs that provide reports in specialized areas, such as tenant screening services (that report to landlords on consumers who have applied to rent apartments) and employment screening services (that report to employers to assist them in evaluating job applicants).

CRAs other than credit bureaus provide many different types of consumer reports. They may report information they have compiled themselves, purchased from another CRA, or both. For example, a tenant screening service may report only the information in its files that it has received from landlords, only a consumer report obtained from another CRA, or a combination of both its own information and resold CRA data, depending on the needs of the business and the information available. Data brokers are subject to the requirements of the FCRA only to the extent that they are providing "consumer reports."

2. "Permissible Purposes" For Disclosure of Consumer Reports

The FCRA limits distribution of consumer reports to those with specific, statutorily-defined "permissible purposes." Generally, reports may be provided for the purposes of making decisions involving credit, insurance, or employment.[14] Consumer reporting agencies may also provide reports to persons who have a "legitimate business need" for the information in connection with a consumer-initiated transaction.[15] Target marketing—making unsolicited mailings or telephone calls to consumers based on information from a consumer report—is generally not a permissible purpose.[16]

There is no general "law enforcement" permissible purpose for government agencies. With few exceptions, government agencies are treated like other parties—that is, they must have a permissible purpose to obtain a consumer report.[17] There are only two limited areas in which the FCRA makes any special allowance for governmental entities. First, the law has always allowed such entities to obtain limited identifying information (name, address, employer) from CRAs without a "permissible purpose."[18] Second, the FCRA was amended to add express provisions permitting government use of consumer reports for counterintelligence and counter-terrorism.[19]

---

[11] What constitutes a "consumer report" is a matter of statutory definition (15 U.S.C. § 1681a(d)) and case law. Among other considerations, to constitute a consumer report, information must be collected or used for "eligibility" purposes. That is, the data must not only "bear on" a characteristic of the consumer (such as credit worthiness, credit capacity, character, general reputation, personal characteristics, or mode of living), it must also be *used* in determinations to grant or deny credit, insurance, employment, or in other determinations regarding permissible purposes. *Trans Union,* 81 F.3d at 234.

[12] The FCRA defines a "consumer reporting agency" as an entity that regularly engages in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

[13] As discussed more fully below, the "permissible purposes" set forth in the FCRA generally allow CRAs to provide consumer reports to their customers who have a legitimate business need for the information to evaluate a consumer who has applied to the report user for credit, employment, insurance, or an apartment rental. 15 U.S.C. § 1681b(a)(3).

[14] 15 U.S.C. § 1681b(a)(3)(A), (B), and (C). Consumer reports may also be furnished for certain ongoing account-monitoring and collection purposes.

[15] 15 U.S.C. § 1681b(a)(3)(F). This subsection allows landlords a permissible purpose to receive consumer reports. It also provides a permissible purpose in other situations, such as for a consumer who offers to pay with a personal check.

[16] The FCRA permits target marketing for firm offers of credit or insurance, subject to statutory procedures, including affording consumers the opportunity to opt out of future prescreened solicitations. 15 U.S.C. § 1681a(c), (e).

[17] For example, a government agency may obtain a consumer report in connection with a credit transaction or pursuant to a court order.

[18] 15 U.S.C. § 681f. The information a government agency may obtain under this provision does not include Social Security numbers.

[19] 15 U.S.C. §§1681u, 1681v.

3. "Reasonable Procedures" to Identify Recipients of Consumer Reports

The FCRA also requires that CRAs employ "reasonable procedures" to ensure that they supply consumer reports only to those with an FCRA-sanctioned "permissible purpose." Specifically, Section 607(a) provides that CRAs must make "reasonable efforts" to verify the identity of prospective recipients of consumer reports and that they have a permissible purpose to use the report.[20]

The Commission has implemented the general and specific requirements of this provision in a number of enforcement actions that resulted in consent orders with the major nationwide CRAs[21] and with resellers of consumer reports (businesses that purchase consumer reports from the major bureaus and resell them).[22] For example, in the early 1990s, the FTC charged that resellers of consumer report information violated Section 607(a) of the FCRA when they provided consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining the data.[23] In settling these charges, the resellers agreed to employ additional verification procedures, including verifying the identities and business of current and prospective subscribers, conducting periodic, unannounced audits of subscribers, and obtaining written certifications from subscribers as to the permissible purposes for which they seek to obtain consumer reports.[24] In 1996, Congress amended the FCRA to impose specific duties on resellers of consumer reports.[25]

In addition to the reasonable procedures requirement of Section 607(a), the FCRA also imposes civil liability on users of consumer report information who do not have a permissible purpose and criminal liability on persons who obtain such information under false pretenses.

B. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act imposes privacy and security obligations on "financial institutions."[26] Financial institutions are defined as businesses that are engaged in certain "financial activities" described in Section 4(k) of the Bank Holding Company Act of 1956[27] and its accompanying regulations.[28] These activities include traditional banking, lending, and insurance functions, as well as other activities such as brokering loans, credit reporting, and real estate settlement services. To the extent that data brokers fall within the definition of financial institutions, they would be subject to the Act.

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of GLBA and its implementing privacy rule[29] from disclosing nonpublic personal information to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[30] However, GLBA provides a number of statutory exceptions under which disclosure is permitted without specific notice to the consumer. These exceptions include consumer reporting (pursuant to the FCRA), fraud preven-

---

[20] 15 U.S.C. §1681e(a).

[21] *Equifax Credit Information Services, Inc.,* 130 F.T.C. 577 (1995); *Trans Union Corp.* 116 F.T.C. 1357 (1993) (consent settlement of prescreening issues *only* in 1992 target marketing complaint; *see also Trans Union Corp. v. FTC,* 81 F.3d 228 (D.C. Cir. 1996)); *FTC v. TRW Inc.,* 784 F. Supp. 362 (N.D. Tex. 1991); *Trans Union Corp.,* 102 F.T.C. 1109 (1983). Each of these "omnibus" orders differed in detail, but generally covered a variety of FCRA issues including accuracy, disclosure, permissible purposes, and prescreening.

[22] *W.D.I.A.,* 117 F.T.C. 757 (1994); *CDB Infotek,* 116 F.T.C. 280 (1993); *Inter-Fact, Inc.,* 116 F.T.C. 294 (1993); *I.R.S.C.,* 116 F.T.C. 266 (1993) (consent agreements against resellers settling allegations of failure to adequately insure that users had permissible purposes to obtain the reports).

[23] *Id.*

[24] A press release describing the consent agreement is available at: http://www.ftc.gov/opa/predawn/F93/irsccdb3.htm.

[25] Resellers are required to identify their customers (the "end users") to the CRA providing the report and specify the purpose for which the end users bought the report, and to establish reasonable procedures to ensure that their customers have permissible purposes for the consumer reports they are acquiring through the reseller. 15 U.S.C. §1681f(e).

[26] 15 U.S.C. § 6809(3)(A).

[27] 12 U.S.C. § 1843(k).

[28] 12 C.F.R. §§225.28, 225.86.

[29] Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

[30] The GLBA defines "nonpublic personal information" as any information that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, Social Security number, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.,* 65 Fed. Reg. 33,646, 33,680 (May 24, 2000) (the FTC's Privacy Rule).

tion, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.[31] Entities that receive information under an exception to GLBA are subject to the reuse and redisclosure restrictions under the GLBA Privacy Rule, even if those entities are not themselves financial institutions.[32] In particular, the recipients may only use and disclose the information "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."[33]

Data brokers may receive some of their information from CRAs, particularly in the form of identifying information (sometimes referred to as "credit header" data) that includes name, address, and Social Security number. Because credit header data is typically derived from information originally provided by financial institutions, data brokers who receive this information are limited by GLBA's reuse and redisclosure provision. For example, if a data broker obtains credit header information from a financial institution pursuant to the GLBA exception "to protect against or prevent actual or potential fraud,"[34] then that data broker may not reuse and redisclose that information for marketing purposes.

2. Required Safeguards for Customer Information

GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers directly or from other financial institutions.[35] The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,[36] requires financial institutions to develop a written information security plan that describes their programs to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires a plan that accounts for each entity's particular circumstances—its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps (for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers) in implementing their plans. Since the GLBA Safeguards Rule became effective in May 2003, the Commission has brought two law enforcement actions against companies that violated the Rule by not having reasonable protections for customers" personal information.[37]

To the extent that data brokers fall within GLBA's definition of "financial institution," they must maintain reasonable security for customer information. If they fail to do so, the Commission could find them in violation of the Rule. The Commission can obtain injunctive relief for such violations, as well as consumer redress or disgorgement in appropriate cases.[38]

C. Section 5 of the FTC Act

In addition, Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[39] Under the FTC Act, the Commission has broad jurisdiction to prevent 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.[40] To date, the Commission has brought five cases against companies for deceptive security claims, alleging that the companies made explicit or implicit promises to take

---

[31] 15 U.S.C. § 6802(e).

[32] 16 C.F.R. § 313.11(a).

[33] *Id.*

[34] 15 U.S.C. § 502(e)(3)(B).

[35] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

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

[37] *Sunbelt Lending Services,* (Docket No. C-4129) (consent order); *Nationwide Mortgage Group, Inc.,* (Docket No. 9319) (consent order).

[38] 15 U.S.C. § 6805(a)(7). In enforcing GLBA, the FTC may seek any injunctive and other equitable relief available to it under the FTC Act.

[39] 15 U.S.C. § 45(a).

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

reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive.[41] The consent orders settling these cases have required the companies to implement rigorous information security programs generally conforming to the standards set forth in the GLBA Safeguards Rule.[42]

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.[43] The Commission has used this authority to challenge a variety of injurious practices.[44]

The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain other specific classes of information. For example, the Driver's Privacy Protection Act ("DPPA")[45] prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance.

The privacy rule under the Health Information Portability and Accountability ("HIPAA") Act allows for the disclosure of medical information (including patient records and billing statements) between entities for routine treatment, insurance, and payment purposes.[46] For non-routine disclosures, the individual must first give his or her consent. As with the DPPA, the HIPAA Privacy Rule provides a list of uses for which no consent is required before disclosure. Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[47]

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

In addition to its regulatory and enforcement efforts, the Commission assists consumers with advice on the steps they can take to minimize their risk of becoming identity theft victims, supports criminal law enforcement efforts, and provides resources for companies that have experienced data breaches. The 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act") provides the FTC with a specific role in combating identity theft.[48] To fulfill the Act's mandate, the Commission implemented a program that focuses on collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; maintaining and promoting the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and providing outreach and education to consumers, law enforcement, and industry.

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive about 15,000 to 20,000 contacts per week on the hotline, or via our website or mail from victims

---

[41] *Petco Animal Supplies, Inc.* (Docket No. C-4133); *MTS Inc., d/b/a Tower Records/Books/Video* (Docket No. C-4110); *Guess?, Inc.* (Docket No. C-4091); *Microsoft Corp.,* (Docket No. C-4069); *Eli Lilly & Co.,* (Docket No. C-4047). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises—enf.html.

[42] As the Commission has stated, 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. 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. *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) (available at http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf).

[43] 15 U.S.C. § 45(n).

[44] 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), 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), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[45] 18 U.S.C. §§2721-25.

[46] 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

[47] 45 C.F.R. §164.530(c).

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

and consumers who want to learn about how to avoid becoming a victim. The callers to the hotline receive counseling from trained personnel who provide information on prevention of identity theft, and also inform victims of the steps to take to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1) obtain copies of their credit reports and have a fraud alert placed on them; (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and, if possible, obtain a police report. A police report is helpful both in demonstrating to would-be creditors and debt collectors that the consumers are victims of identity theft, and also serves as an "identity theft report" that can be used for exercising various rights under the newly enacted Fair and Accurate Credit Transactions Act.[49] The FTC's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaint into the Clearinghouse.[50]

The FTC has also taken the lead in the development and dissemination of consumer education materials. To increase awareness for consumers and provide tips for minimizing the risk of identity theft, the FTC developed a primer on identity theft, *ID Theft: What's It All About?* Together with the victim recovery guide, *Take Charge: Fighting Back Against Identity Theft,* the two publications help to educate consumers. The FTC alone has distributed more than 1.4 million copies of the *Take* Charge booklet since its release in February 2000 and has recorded more than 1.7 million visits to the Web version. The FTC's consumer and business education campaign includes other materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

The Commission has also developed ways to simplify the recovery process. One example is the ID Theft Affidavit, which is included in the Take Charge booklet and on the website. The FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. To date, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit and has recorded more than 709,000 hits to the Web version.

B. Working with Law Enforcement

A primary purpose of the Identity Theft Act was to enable criminal law enforcement agencies to use a single database of victim complaints to support their investigations. To ensure that the database operates as a national clearinghouse for complaints, the FTC accepts complaints from state and federal agencies as well as from consumers.

With almost 800,000 complaints, the Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the prevalence of identity theft complaints by states and cities.[51] Law enforcement and policy makers use these reports to better understand identity theft.

Since the inception of the Clearinghouse, more than 1,100 law enforcement agencies have signed up for the database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week.

The Commission also encourages even greater use of the Clearinghouse through training seminars offered to law enforcement. Beginning in 2002, the FTC, in cooperation with the Department of Justice, the U.S. Postal Inspection Service, and the U.S. Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, this group has held 16 seminars across the country. More than 2,200 officers have attended these seminars, representing over 800 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse. The staff then refers the investigative reports to Finan-

---

[49] These include the right to an extended, seven-year fraud alert, the right to block fraudulent trade lines on credit reports, and the ability to obtain copies of fraudulent applications and transaction reports. *See* 15 U.S.C. §1681 *et seq.,* as amended.

[50] Once a consumer informs a consumer reporting agency that the consumer believes that he or she is the victim of identity theft, the consumer reporting agency must provide the consumer with a summary of rights titled "Remedying the Effects of Identity Theft" (available at http://www.ftc.gov/bcp/conline/pubs/credit/idtsummary.pdf).

[51] Federal Trade Commission—National and State Trends in Fraud & Identity Theft (Feb. 2004) (available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf).

cial Crimes Task Forces and other law enforcers for further investigation and potential prosecution.

C. Working with Industry

The private sector can help tackle the problem of identity theft in several ways. From prevention of identity theft through better security and authentication, to helping victims recover, businesses play a key role in addressing identity theft.

The FTC works with institutions that maintain personal information to identify ways to keep that information safe from identity theft. In 2002, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to a roundtable discussion of what steps entities can and do take to prevent identity theft and ensure the security of personal information in employee and customer records. This type of informal event provides an opportunity for the participants to share information and learn about the practices used by different entities to protect against identity theft.

The FTC also provides guidance to businesses about information security risks and the precautions they must take to protect or minimize risks to personal information. For example, the Commission has disseminated guidance for businesses on reducing risks to their computer systems,[52] as well as guidance for complying with the GLBA Safeguards Rule.[53] Our emphasis is on preventing breaches before they happen by encouraging businesses to make security part of their regular operations and corporate culture. The Commission has also published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business,* which is a business education brochure on managing data compromises.[54] This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

V. CONCLUSION

Data brokers collect and distribute a wide assortment of consumer information and may therefore be subject to a variety of federal laws with regard to the privacy and security of consumers' personal information. Determining which laws apply depends on the type of information collected and its intended use. The Commission is committed to ensuring the continued safety of consumers' personal information and looks forward to working with you to explore this subject in more depth.

Mr. STEARNS. I thank the Madam Chairman for her opening statement. I will start with my questions. And it might be helpful, in light of your opening statement, to indicate in your answers whether this is your personal opinion, or whether this is the policy of the Federal Trade Commission, if it turns out that is the case.

And if you don't mind, I would like you just to give a yes or no here. Should Congress prohibit the disclosure of Social Security numbers without consumers' prior consent? Just yes or no.

Ms. MAJORAS. I will try, Congressman Stearns. I——

Mr. STEARNS. Well, we can go back to this, but you know, as—dealing with these hearings, I like to put people right on the spot, just yes or no.

Ms. MAJORAS. I understand, but I am afraid on that one, I have to answer I can't absolutely answer yes.

Mr. STEARNS. Because you are saying there is extenuating circumstances.

Ms. MAJORAS. Absolutely.

Mr. STEARNS. Okay. Okay. I will accept that. Would you say that Social Security numbers that appear on credit headers should be truncated?

Ms. MAJORAS. It depends on what they are used for.

---

[52] *Security Check: Reducing Risks to Your Computer Systems,* available at http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

[53] *Financial Institutions and Customer Data: Complying with the Safeguards Rule,* available at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[54] *Information Compromise and the Risk of Identity Theft: Guidance for Your Business,* available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.

Mr. STEARNS. Okay. So in your—like the Chairman Barton talked about, the Social Security number, and other members are saying it is your personal property, so you are saying that Congress should not prohibit the disclosure of Social Security numbers in some cases?

Ms. MAJORAS. Well, that is correct.

Mr. STEARNS. Okay.

Ms. MAJORAS. I don't think that would be valuable to consumers——

Mr. STEARNS. Okay. So there is a tipping point, then, you are saying, where they get much more information of a consumer, and where that Social Security number would be conclusive enough that it should be——

Ms. MAJORAS. No question there is a line drawing.

Mr. STEARNS. Okay. In your—you have indicated that there should be a comprehensive Federal law dealing with privacy and security of consumer information. That is correct, right?

Ms. MAJORAS. Yes.

Mr. STEARNS. And is that your personal opinion, or the Federal Trade Commission?

Ms. MAJORAS. It is not in my written testimony, so I will have to say that it is my opinion that we can extend some of the Federal laws in place today, and regulations, much more broadly.

Mr. STEARNS. Beyond the Gramm-Leach-Bliley Act——

Ms. MAJORAS. Correct.

Mr. STEARNS. [continuing] and beyond the Sarbanes-Oxley, you think there is another role for the Federal Government, dealing with privacy and security. And I have a privacy bill, so I am sympathetic to what you say.

Ms. MAJORAS. Yes.

Mr. STEARNS. But I am just trying to—should consumers have the right to inspect information maintained about them by data brokers, and seek correction of errors in that information?

Ms. MAJORAS. It depends on what the data bank is being used for. If it is a fraud data bank, for example, we wouldn't want fraudsters to be able to see the information collected on them, for example.

Mr. STEARNS. But a lot of people would argue that just like with a credit report, you can call the credit company and say, what does a credit report look like on me, and I think I should have the right, which you do today, to correct it.

Ms. MAJORAS. Yes.

Mr. STEARNS. So following that line of reasoning, why wouldn't consumers have the right to inspect this information that is maintained by data brokers, and seek correction of errors if there are some?

Ms. MAJORAS. And they do, in fact, if data brokers like ChoicePoint are providing information that is considered to be consumer report information under the statute.

Mr. STEARNS. California has a law dealing with disclosure to consumers, and of course, because of that law, that made ChoicePoint have to notify these 146,000. That is extremely time-consuming. It is difficult if they can find all these people, but we can envision 50 States now starting to pass their own laws, 49 others. Should there

be a nationwide requirement for disclosure, sort of a preemption that the Federal Government does, so that all companies like ChoicePoint, LexisNexis, deal with this Federal law, and not have to deal with 50 separate laws?

Ms. MAJORAS. Yes. A Federal requirement would be appropriate when there is a significant risk to consumers from the breach.

Mr. STEARNS. Okay. There is some talk about some people saying we should—we are now—and we need a Communications Bill of Rights, that specifies what a person dealing in this new information technology age, he or she has a consumer—a Communications Bill of Rights. Do you see anything like that through the Federal Trade Commission?

Ms. MAJORAS. I am sorry, not particularly something we are calling the Communications Bill of Rights.

Mr. STEARNS. But what are you calling it then?

Ms. MAJORAS. I am—I want to make sure I am clear on what you are talking about. Are you talking about communication between a consumer and, for example, a financial institution?

Mr. STEARNS. Yes. Well, dealing with a data base, and dealing with—what are the rights of the consumers, in terms of whether they opt in, opt out, and that is my next question, whether you would favor it within this, an opt-in or opt-out provision.

Ms. MAJORAS. First and foremost, we believe consumers want to be sure that their personal information is safeguarded. We think that is—that security is what consumers are first and foremost concerned about, and that they do have the right to ensure that those companies that have their information are safeguarding it appropriately. No question about that.

With respect to opt-in or opt-out, I think it is important that we learn from the Gramm-Leach-Bliley scheme. What we have found is that, in fact, consumers have received millions collectively of notices of their right to opt out of a financial institution sharing their personal information, and they have not exercised that right. They have not wanted to bother with that. We believe, again, they really want to just make sure that banks and merchants and others are responsibly handling their information and safeguarding it.

Mr. STEARNS. Going back to my first question, should Congress prohibit the disclosure of Social Security numbers without consumers' prior consent. You could not answer that yes or no. Can you give me a sentence to answer that? A couple sentences.

Ms. MAJORAS. Okay. Social Security numbers are used for permissible purposes, like matching a particular consumer to a particular credit report, for example, and for verifying accuracy of credit reports, which is something we have talked about here today already. And those are important purposes, because there is no other unique identifier for U.S. citizens. So the key is to not squelch use of Social Security numbers for purposes for which consumers would want to—would want that use, because in fact, consumers care a lot about things like instant credit, and that is also important.

But one more sentence, I promise, Mr. Congressman, Mr. Chairman. We believe there are instances in which Social Security numbers may be asked for or shared just simply out of habit, where

they are really not necessary, and there, we should be looking at whether further restriction would be appropriate.

Mr. STEARNS. Okay. My time has expired, but I would interpret what you say, that should Congress prohibit the disclosure of Social Security numbers without consumers, is you would say no, they should not prohibit. That is what I interpreted.

The ranking member, Ms. Schakowsky.

Ms. SCHAKOWSKY. Thank you. Welcome, Chairman Majoras.

Ms. MAJORAS. Thank you.

Ms. SCHAKOWSKY. Illinois just became eligible—Illinoisans just became eligible to get free credit reports under a program, I think, administered by you, that we can now get that information. And it is pretty widely known, and I would assume, pretty widely used, that consumer—is that correct?

Ms. MAJORAS. Yes, ma'am.

Ms. SCHAKOWSKY. People are doing that. But I am wondering how many consumers really know about data brokers? You know, we all know about credit agencies and about our credit reports, but do you think most consumers actually know about data brokers?

Ms. MAJORAS. Until recently, no. I don't believe so.

Ms. SCHAKOWSKY. I don't think so either. And so, I think that this—the revelation that this information is out there, and has been—that security has been breached has really been an eye-opener, I think, for a lot of people, and I think appropriately, now, the Congress is looking on where it fits in.

And one of the questions I had, as I said in my opening statement, the 1974 Privacy Act, I thought, said that the—acknowledged the power of this aggregated information, and made it illegal for government agencies to amass the kind of personal information that it seems to me that data brokers do. And yet, the government agencies, how many are they, that actually purchase this information from data brokers? So it seems to me that from the government standpoint alone, that that is, if not a breach of the actual language of the law, the spirit of the law, in saying that well, we can't do that kind of data collection, but we will actually purchase it, and then, that is further problematic, because that information is not—there is no safeguards that it is even accurate.

I wanted your response, in relation to the 1974 law.

Ms. MAJORAS. Well, it is true that government agencies use information that has been compiled by data brokers, and we need to remember that the reason they use it is if there is a strong need in tracking down deadbeats who have not paid their child support, or in tracking down those, you know, criminals. There is a need for information like that, and that is why, as I understand it, government agencies have been using data brokers.

Now, I don't enforce that statute, obviously, against government agencies, and so I don't have a personal opinion on the application of that statute. But I do wholeheartedly agree with you that consumers have the right to ensure that the information is safeguarded, and certainly, for the types of information that data brokers are collecting, that is being used for eligibility decisions on consumers, then data brokers should be following the Fair Credit Reporting Act, which does require certain standards for accuracy and the like.

Ms. SCHAKOWSKY. So who assures that that happens? If consumers are unaware, actually, of the existence of these data brokers, and if that information, then, is used to deny them credit, for example, how do they—how would they know that?

Ms. MAJORAS. Well, there are certain requirements under the FCRA that accompany—that is giving out the information is required to follow. So if, for example—so any company that is supplying consumer report information, and that is, generally, information that is being used to make eligibility determinations, has some requirements that it must follow, but it is true that unlike with respect to the three credit reporting agencies, who I agree with you, most consumers know about, I don't know that at least to date, consumers have known about these data brokers.

Ms. SCHAKOWSKY. So if I am applying for a loan, and the financial institution is going to one of these data brokers for the information, am I supposed to get notified that that is the source of the information, that the data broker is the source of the information? And does that ever happen?

Ms. MAJORAS. I don't believe you would be notified of the source of the information, no. I can't think of an—in this patchwork of laws we have, I can't think of one requiring in particular——

Ms. SCHAKOWSKY. I am confused about what this notification provision is for credit reporting agencies, for example. What are you saying?

Ms. MAJORAS. Well, if information on your credit report is used, and an adverse determination is made on that, then a consumer——

Ms. SCHAKOWSKY. Is notified at their home.

Ms. MAJORAS. [continuing] is notified—would have to be notified that they have been denied on the basis of that information.

Ms. SCHAKOWSKY. Is that the responsibility of the financial institution, rather than the credit reporting agency?

Ms. MAJORAS. I believe it is the financial institution.

Ms. SCHAKOWSKY. Okay. So do we know that they are, in fact, if they are using this other source of information, are they regularly telling consumers that it is, you know, ChoicePoint or whatever, that it is the basis—on that basis, you are being denied?

Ms. MAJORAS. They are being notified that they are being—that it was on the basis of what has been supplied in their consumer report. I don't know whether they are notified as to which credit reporting agency or private data broker. I just don't know the answer.

Ms. SCHAKOWSKY. Obviously, there is a lot of holes that we need to be filling in. Thank you.

Ms. MAJORAS. It is very complicated. Thank you.

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

Chairman BARTON. Thank you, Mr.—Chairman Stearns. Madam Chairwoman, I just have two questions.

Is there any reason that we should not make it illegal to share or trade a person's Social Security number, and the data that goes with it, without their permission?

Ms. MAJORAS. There are a couple of reasons why, and that is, in the context of, for example, a transaction in which the consumer is attempting to get credit or a loan.

Chairman BARTON. I said without their permission.

Ms. MAJORAS. Right. So if they—if it is being provided. The only other place I can think of, Chairman Barton, is with respect to tracking down criminals. And if we are tracking down criminals, and trying to match criminals, like, for example, identity thieves, that might be another area where we would want to consider——

Chairman BARTON. So a law enforcement exception, and then, when you give permission, in order to get something of value to you, that they can check on you, and—so—but other than that, you would support a law that Social Security number can't be used, period, without your permission?

Ms. MAJORAS. I think we would want to take a closer look to all the exceptions. For example, in Gramm-Leach-Bliley, which are very similar to the law enforcement exceptions, to make sure that we are not missing something. But in terms of—for marketing purposes, or——

Chairman BARTON. But under Gramm-Leach-Bliley, all they have to do is tell you they are doing it. They don't have to get your permission.

Ms. MAJORAS. Well, that is right, and they give you the ability to opt out, but there are some exceptions in Gramm-Leach-Bliley, where they don't even have to give you the chance to opt out, and those are the exceptions, I think, that we ought to look at closely, in the same context.

Chairman BARTON. What would the Federal Trade Commission's response be to requiring that if your personal information is stolen, as has been—has happened in these two instances, that at a minimum, the company that had the information compromised would have to notify the individual that their information has been stolen or compromised?

Ms. MAJORAS. If the information that has been stolen or compromised puts the consumer at significant risk, then we think that the company should be required to take reasonable steps to provide notice to consumers.

Chairman BARTON. Take reasonable steps. Define reasonable steps.

Ms. MAJORAS. Well, it all depends on the circumstances. Consumers move around, and so the question is, how—really, the question is only to what degree does the company need to spend time trying to track down that individual.

Chairman BARTON. What if we said reasonableness is the same standard as if you were trying to collect a bill from that individual?

Ms. MAJORAS. Well, that would be something that most companies would be very familiar with. Probably a good——

Chairman BARTON. Well, they—see—you know——

Ms. MAJORAS. Probably a good starting point, Chairman.

Chairman BARTON. Okay. Just a second. Staff would like me to ask you about your—under Gramm-Leach-Bliley, one of the exceptions is for fraud prevention, and my understanding is that the ChoicePoint identity theft, or the theft of the material, the company, the individuals, falsely portrayed themselves to be a corporation that was trying to get information to prevent fraud.

So is that something that we need to tighten up, the—either eliminate as an exception, or tighten up the conditions under which you could use that exception?

Ms. MAJORAS. Well, I think we should take a very close look at the exception, and make sure it is not swallowing the rule, but in addition, in this instance, we also need to look, I think, at extending the Commission's Safeguards Rule, so that all companies, like consumer reporting agencies, are required to take certain steps when information is requested, so that they are not just selling it to anyone, but they are, in fact, selling it to someone who has a permissible purpose. That is the other way we could tighten.

Chairman BARTON. All right. And I guess my final question, in general, would it be the Federal Trade Commission's position that Federal legislation of some sort is necessary and helpful in this area?

Ms. MAJORAS. Yes, that is my position.

Chairman BARTON. Okay. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. The gentlelady from Wisconsin. Oh, the gentleman from Massachusetts. Yes.

Mr. MARKEY. Thank you, Mr. Chairman. Madam Chairlady, in the prepared testimony submitted by the Electronic Privacy Information Center, EPIC, Marc Rotenberg states that back on December 16, 2004, EPIC urged the FTC to investigate ChoicePoint and other data brokers for possible violations of the Federal privacy laws.

Did the FTC initiate any investigation into ChoicePoint in response to this request?

Ms. MAJORAS. The EPIC petition asked us to examine whether existing laws provided adequate regulation and oversight over companies like ChoicePoint, a very important question.

We actually had been looking at the issue before we received the EPIC petition. When we received the EPIC letter, we increased our efforts, and as you may have heard, we have recently been able to publicly acknowledge that we have, in fact, opened an investigation of ChoicePoint.

Mr. MARKEY. But had you officially begun an investigation before press reports appeared, indicating that there had been security breaches at ChoicePoint?

Ms. MAJORAS. No, we had no evidence that ChoicePoint had violated the law at that point.

Mr. MARKEY. You did not believe that EPIC's information was sufficient to trigger an investigation?

Ms. MAJORAS. We thought EPIC's information was sufficient to look at the entire landscape, to see if new regulation or law was necessary.

Mr. MARKEY. And what was deficient in EPIC's information? What was lacking that you feel was—that would have been necessary to trigger an investigation?

Ms. MAJORAS. I am sorry, sir, because I have an active investigation of ChoicePoint, I am afraid I can't talk further about their actual conduct in the public forum.

Mr. MARKEY. The point I am trying to make here is that I think that there was a warning, that there was information at the Federal Trade Commission, that the Federal Trade Commission has to

be much more aggressive than it has been in the pursuit of the protection of the privacy of individuals, and this is a perfect example of where the Federal Trade Commission was not as aggressive as the American people would expect you to be.

Now, as I understand it, ChoicePoint maintained some data bases of credit reports that would be regulated under the Fair Credit Reporting Act, but that it also had other data bases of information that did not meet the Federal Credit Reporting Act's definition of a credit report. Is that right?

Ms. MAJORAS. That is my understanding from public sources, yes.

Mr. MARKEY. And this information may have been amongst the information that was compromised. Is that right?

Ms. MAJORAS. That is my understanding, again, from press reports.

Mr. MARKEY. Now, a Social Security number is not considered a credit report, and also, isn't protected under the Federal Credit Reporting Act? Is that also correct?

Ms. MAJORAS. Correct.

Mr. MARKEY. So don't we really need a new law that regulates these information brokers, so that we have fair information practices in place to protect the public?

Ms. MAJORAS. I think we could use new law that focuses on misuse and absolutely focuses on the security of sensitive information, yes.

Mr. MARKEY. Shouldn't we ban the commercial sale of Social Security numbers?

Ms. MAJORAS. It depends on what they are being used for.

Mr. MARKEY. If they are just being used in a way that allows my neighbors to gain access to my Social Security number, shouldn't that be banned?

Ms. MAJORAS. Yes, absolutely.

Mr. MARKEY. Should BJ's Wholesale have the ability to get my Social Security number?

Ms. MAJORAS. Well, it all depends on what they are using it for, and consumers, of course, part with their Social Security number, indeed, to be able to buy goods and services, or to get credit, for example.

Mr. MARKEY. But should they be able to obtain it, if I haven't given it to them?

Ms. MAJORAS. They might—we might want them to be able to obtain it, for example, from a credit reporting agency, if they are trying to verify, for example, that I am who I say I am, and so that is something we need to look at closely. But certainly, banning misuse and purposes outside a window, absolutely.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Mr. Murphy.

Mr. MURPHY. Thank you, Mr. Chairman. A couple of quick questions. First of all, if we do nothing here in correcting some of these patterns, what do you anticipate the level this will grow to in 5 or 10 years?

Ms. MAJORAS. My goodness. I don't know that I can speculate. I am—we try to look for good news wherever we can find it. This isn't much good news, but at least between—from what we can tell,

between 2003 and 2004, the number of identity theft victims didn't grow. We hope that is because some of the steps that we have been able to take under our authority, and that banking agencies have been taking, and of course, merchants and responsible companies, are having some impact. But it is—we do believe that more needs to be done to safeguard personal information.

Mr. MURPHY. My point is, do you believe that there will be a number of technological advances that companies will make in order to safeguard things on their own, or I am thinking your testimony did not contain references to legislation needed to protect consumers' security and privacy. So I am wondering if you think that the current Federal law regarding data security and privacy is adequate to protect consumers.

Ms. MAJORAS. Yes, sir. As I said in my oral remarks, we think there are two places where we should start with respect to new legislation, perhaps. The first is extending the Commission's GLB Safeguards Rule beyond financial institutions, to include far more institutions that collect or disseminate personal data.

And the second would be to consider a Federal requirement for notice when there have been security breaches that pose a significant risk to consumers.

Mr. MURPHY. All right. Thank you. And I want, you know, I appreciate the work you are doing, to make sure you continue on with an investigation that is protecting consumers. Thank you very much.

And thank you, Mr. Chairman.

Ms. MAJORAS. Thank you.

Mr. STEARNS. I thank the gentleman. The gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman, and thank you for your testimony today.

I wanted to probe just a little bit more with the reasonableness standard that was being discussed earlier. Under the Fair Credit Reporting Act, it would also—Gramm-Leach-Bliley—companies have a duty to take, or make reasonable efforts to verify both the identity of prospective recipients of consumer reports, and they also have to make reasonable efforts to make sure that these prospective recipients have a permissible purpose.

Without getting into the details of any open investigation, could you make this real for us by giving some examples of what the Commission views as reasonable efforts?

Ms. MAJORAS. Okay. Yes.

We—and we have entered into some consent agreements with companies over time, in which we have laid out, in fact, what needs to be done. Now, in the statute itself, there are requirements that a CRA that falls under the statute must require certification of the identity, and certification of the permissible purpose. That is one. Beyond that, there are other things that can be done, and we understand are done, at times, by CRAs, like audits, and like onsite drop-in visits. And audits of the actual information as it is going out, and to whom it is going to. Those are some of the measures.

Ms. BALDWIN. Okay. And quickly, I wanted to note the efforts undertaken by the Commission under the Identity Theft Act, to provide consumers with information and assistance, and particu-

larly, assistance to victims of identity theft. I also appreciate the Commission's leadership in providing educational materials to increase consumer awareness about the problem of identity theft.

I am wondering, in that arena, do you feel that the Commission has sufficient statutory authority to provide any services deemed necessary or advisable under that law?

Ms. MAJORAS. I think we do, and we will continue to educate consumers, and help any consumers who have fallen victim, and of course, what we really want to do is educate consumers in advance, because there are a number of things that consumers can do to at least decrease the risk.

It is always a matter of resources. We are a small agency, and I think we are doing a lot in stretching our dollars. I think our efforts in education and in training of law enforcement have been greatly appreciated. I recently received an email from a local police officer, talking about how much they appreciate our educating them, because of course, they are the first line in this. We don't have criminal enforcement authority against this crime. We are facilitating the prosecution of these thieves, and we are obviously facilitating education.

Mr. BALDWIN. Thank you.

Mr. STEARNS. I thank the gentlelady. We have one vote, and then we—I am going to come right back. So we are going to recess the committee for this one vote, and with your patience, if you will stay with us, and I will start immediately, and I will urge members to come back quickly, and there is about 7 minutes before we have—they shut down the vote, so I will be right back.

Ms. MAJORAS. Thank you, Mr. Chairman.

[Recess.]

Mr. STEARNS. The subcommittee will reconvene, and the gentleman from New Hampshire, Mr. Bass, is recognized.

Mr. BASS. Thank you very much, and I would just like to ask some basic questions, if I could.

Could you tell the committee, the subcommittee exactly what a credit bureau is, and do they sell consumers' information?

Ms. MAJORAS. Forgive me. A credit bureau is a company that collects information regarding consumers, generally speaking, so that it can be compiled and sold, so that merchants, banks, and insurance companies and the like can make eligibility determinations about consumers.

Mr. BASS. Do consumers have the ability to opt out of information collection by credit bureaus?

Ms. MAJORAS. They do not.

Mr. BASS. Do credit bureaus sell information to entities like ChoicePoint and LexisNexis, and is there Federal supervision by a regulator of the downstream use of information sold by credit bureaus to data brokers?

Ms. MAJORAS. Yes, there is some, so yes, they do sell the information, and yes, there is some Federal supervision under the Fair Credit Reporting Act.

Mr. BASS. Is there Federal supervision by a regulator of the subsequent sale of consumers' information by a data broker to other businesses?

Ms. MAJORAS. It depends on what kind of information they are selling. If it is a consumer report, for example, that they are reselling, which they originally got from a CRA, then the answer is yes, then they must comply with the requirements of the FCRA. There may be other information, however, that data brokers collect, in fact, I believe there are, that are not subject to the requirements of the FCRA.

Mr. BASS. Could you explain "permissible purposes" for which consumer reports can be disclosed under the Fair Credit Reporting Act?

Ms. MAJORAS. It—generally, a permissible purpose is to determine a consumer's eligibility for credit, for insurance, for employment, and the like.

Mr. BASS. You have testified that, "targeted marketing is generally not a permissible purpose." When is targeted marketing permissible?

Ms. MAJORAS. There is an exception in the statute with respect to prescreened offers.

Mr. BASS. Has the FTC brought any enforcement cases against firms who have used credit reports for targeted marketing?

Ms. MAJORAS. No.

Mr. BASS. Okay. I yield back, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Madam Chairman, we would like to thank you very much for your patience and for attending. We are now going to call up the second panel.

Ms. MAJORAS. Okay. Thank you very much, Mr. Chairman.

Mr. STEARNS. We have Mr. Kurt Sanford, President and Chief Executive Officer of U.S. Corporate and Federal Government Markets, LexisNexis; Mr. Derek Smith, Chairman and CEO of ChoicePoint; Mr. Joseph—no, excuse me, that is just the two. So we are—just those two on the second panel, and we are going to let you start your opening statement.

We have about 12½ minutes to a vote, so I was hoping we could tear through this, so when we come back, this is a surprise vote, we can start on the questions.

So Mr. Sanford, I will let you start with your opening statement. Just make sure the mike is close to you, and it also is turned on.

STATEMENTS OF KURT P. SANFORD, PRESIDENT AND CHIEF EXECUTIVE OFFICER, U.S. CORPORATE AND FEDERAL GOVERNMENT MARKETS, LEXISNEXIS; AND DEREK SMITH, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CHOICEPOINT, INC.

Mr. SANFORD. Good morning, Chairman Stearns and other distinguished members of the subcommittee. My name is Kurt Sanford. I am the Chief Executive Officer for Corporate and Federal Markets at LexisNexis. I appreciate the opportunity to be here today to discuss the important public policy issues associated with cybercrime, identity theft, and the protection of consumer information. LexisNexis commends the subcommittee for its leadership on these important issues.

LexisNexis is a leading provider of authoritative legal, public records, and business information. Today, over 3 million professionals, law enforcement officials, government agencies, financial

institutions, and others, subscribe to the LexisNexis services. LexisNexis plays a vital role in supporting government and business customers, who use our information services for important uses, including preventing identity theft and fraud, locating suspects, preventing and investigating terrorist activities, and locating missing children.

LexisNexis is committed to the responsible use of personally identifiable information. We have stringent privacy policies and security measures in place to protect the consumer information in our data bases. We share the subcommittee's concern about the potential misuse of this information to commit identity theft and fraud. We look forward to sharing our views on possible ways to further enhance information security, and address the growing problems of cybercrime and identity theft.

I would like to take a few minutes to discuss data security incidents announced last week at Seisint, the information company we acquired last September. As part of the integration of Seisint with LexisNexis, we are conducting a thorough review of the company's verification, authorization, and security procedures and policies. During that process, a LexisNexis integration team became aware of some billing irregularities with several customer accounts. Upon further investigation, the team detected some unusual usage pattern within these accounts. The team then informed senior management, and I contacted the United States Secret Service.

The incident is still being investigated, but it appears that cybercriminals compromised IDs and passwords of legitimate Seisint customers, and used those IDs and passwords to access public records and certain personally identifying information, such as Social Security numbers and driver's license numbers.

No personal financial, credit, or medical information was involved, because Seisint does not collect or sell information of this type. Because this is an ongoing law enforcement investigation, the U.S. Secret Service has asked us to refer all questions regarding the investigation to them. We sincerely regret this incident and any adverse impact that this crime may have upon the individuals whose information was accessed. We have already begun to take steps to assist the affected consumers.

First, based on the investigation to date, we are in the process of notifying approximately 32,000 individuals whose personal information may have been accessed. We expect to complete mailing notices by March 16. Second, we are providing all individuals with a consolidated report, containing information from the three major credit bureaus, and credit monitoring services for 1 year. Third, for those individuals who do become victims of fraud as a result of this incident, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity.

I would like to take a minute to discuss the security systems at LexisNexis and the specific steps we are taking to prevent any future incidents. LexisNexis has long recognized the importance of undertaking extensive measures to protect the information in our data bases, and has a comprehensive security program. Maintaining security is not a static process, but rather, involves continuously evaluating and adjusting our security program.

LexisNexis has physical, administrative, and technical measures to protect the security of information it maintains. Our data facilities are physically secure, and are monitored 24 by 7. Administratively, we have policies and procedures in place to prevent and detect employee misuse of our systems. In addition, we limit a customer's access to sensitive information, according to the purposes which they seek to use the information. Our Chief Privacy Officer and Privacy and Policy Review Board work together to help protect the privacy of information contained in our data bases.

We also undertake regular assessments by independent third parties of both our privacy and security practices. In addition to these security safeguards, LexisNexis has a multilayer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information. Only those customers with a permissible purpose under Federal law are granted access to sensitive data, such as driver's license number and Social Security numbers.

LexisNexis plans to further restrict access to the most sensitive data elements by extending the more restrictive Social Security number truncation policy currently in place for LexisNexis to its recently acquired Seisint business, and by adding a policy to include the masking of driver's license numbers. We are also enhancing ID and password administration procedures. These steps are part of the ongoing review that LexisNexis has undertaken on security practices and procedures and privacy policies across its businesses.

I would like to focus the remainder of my time on policy issues being considered to further protect consumer information. While there are various laws currently in place that govern the collection and distribution of personally identifiable information, we recognize that additional legislation may be necessary to address the growing problem of cybercrime and identity theft.

LexisNexis would support the following legislative approaches. First, consistent with the proposal outlined by FTC Chairman Majoras in her testimony, we support requiring notification in the event of a security breach, where there is a substantial risk of harm to consumers. We share the concerns that Chairman Majoras raised in her testimony about ensuring that there is an appropriate threshold for when consumers actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that is it important that any such proposal contain Federal preemption.

Second, we would support the adoption of data security safeguards, modeled after the Safeguard Rule of the Gramm-Leach-Bliley Act. I understand that the FTC is supportive of this approach as well.

And finally, we strongly encourage legislation that imposes more stringent penalties for identity theft and cybercrimes. Additionally, consumers and industry alike would benefit from an enhanced training for law enforcement, and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and fraud.

It is critical that any legislation being considered ensure that legitimate businesses, government agencies, and other organizations continue to have access to identifying information that they depend

on for important purposes, including fraud detection and prevention, law enforcement, and other critical applications. Moreover, legislation must strike the right balance between security, protecting privacy, and ensuring continued access to critically important information that is provided through information service providers.

Thank you again for the opportunity to be here today to provide the subcommittee with our company's perspective on these important public policy issues. We look forward to working with the subcommittee as it develops proposals to help protect consumers and help fight cybercrime and identity theft. Thank you.

[The prepared statement of Kurt P. Sanford follows:]

PREPARED STATEMENT OF KURT P. SANFORD, PRESIDENT AND CEO, U.S. CORPORATE AND FEDERAL GOVERNMENT MARKETS, LEXISNEXIS

INTRODUCTION

Good morning. My name is Kurt Sanford. I am the Chief Executive Officer for Corporate and Federal Markets at LexisNexis, a division of Reed Elsevier Inc. On behalf of LexisNexis, I appreciate the opportunity to be here today to discuss the important public policy issues associated with the protection of consumer information, cybercrime, and identity theft. LexisNexis commends the Subcommittee for its leadership on these important issues.

LexisNexis is a leading provider of authoritative legal, public records, and business information. Today, over three million professionals—lawyers, law enforcement officials, government agencies, financial institutions and others—subscribe to the LexisNexis services. Government agencies at all levels, businesses, researchers, and others rely on LexisNexis to carry out important functions in our society. LexisNexis Risk Management unit plays a vital role in supporting government and business customers who use our information services for a variety of important uses.

The following are examples of some of the important ways in which the services of LexisNexis are used by customers:

- *Prevent identity theft and fraud*—Banks and other financial institutions routinely rely on personally identifying information contained in LexisNexis' databases to verify the identities of individuals and businesses and prevent identity theft and fraud. For example, LexisNexis has partnered with the American Bankers Association to enable banks and other customers to prevent money laundering and ensure compliance with applicable laws by helping the banks determine if they are doing business with legitimate businesses and consumers. The use of this information by financial institutions to verify and validate information on prospective customers is critical to the success of that program. With the help of LexisNexis, major banks and bank card issuers have experienced significant reductions in dollar losses due to fraud, holding down costs charged to consumers. Special investigation units of insurance companies have experienced similar successes through the use of information in our databases.
- *Locating suspects and helping make arrests*—Many federal, state and local law enforcement agencies rely on LexisNexis to help them locate criminal suspects and to identify witnesses to a crime. For example, Seisint products were used during the course of the D.C. sniper investigation and helped lead to the arrest of the suspects.
- *Preventing and investigating terrorist activities*—Information service providers like LexisNexis offer important tools in the battle against terrorism. Our data, technology, and policy expertise has been instrumental in detecting and preventing terrorist activities.
- *Locating and recovering missing children and assisting in the enforcement of child support obligations*—For many years, LexisNexis has partnered with the National Center for Missing and Exploited Children to help that organization locate missing and abducted children. Locating a missing child within the first 48 hours is critical to success in the recovery effort. The NCMEC has told us that information from LexisNexis has been critical in the Center's successful recovery of many children. In addition, public and private agencies rely on information provided by LexisNexis to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for Enforcement of Support (ACES), a

private child support recovery organization, has had tremendous success in locating nonpaying parents using LexisNexis.

LexisNexis is committed to the responsible use of personally identifiable information and to the protection of consumer privacy. We share the Subcommittee's concern about the potential misuse of this information to commit identity theft and fraud. We look forward to sharing our views on possible ways to further enhance information security and address the growing problems of cybercrime and identity theft.

THE PENDING INVESTIGATION OF THE SEISINT SECURITY INCIDENTS, LEXISNEXIS' RESPONSE AND CYBERCRIME IMPLICATIONS

Before I proceed, I would like to take a few minutes to discuss the data security incidents we recently discovered at Seisint, the information company we acquired last September.

As part of LexisNexis integration of Seisint, we have been conducting a thorough review of the company's verification, authorization, and security procedures and policies. During that process, a LexisNexis integration team became aware of some billing irregularities within several customer accounts. Upon further investigation, the team detected within those accounts some unusual usage patterns. The team then informed senior management and we contacted the United States Secret Service. The U.S. Secret Service was notified because of its well-known expertise in investigating cybercrime and because of its national High Tech Crime Task Force, in which LexisNexis participates.

The incidents are still being investigated, but it appears that cybercriminals compromised IDs and passwords of legitimate Seisint customers and used those IDs and passwords to access certain Seisint databases. The information accessed was limited to public record information and certain identifying information, such as social security numbers and driver's license information. No personal financial, credit, or medical information was involved because Seisint does not collect or distribute information of this type.

We take these incidents very seriously. LexisNexis has long been committed to the protection of consumer privacy and security. We sincerely regret that these criminals were able to fraudulently access this information. We further regret any adverse impact that this crime may have upon the individuals whose information was accessed. We have already begun to take steps to assist individuals whose information may have been accessed. First, based on the investigation to date, we are in the process of notifying approximately 32,000 individuals whose personal information may have been accessed and we expect to complete mailing notices by March 16. Second, we will be providing all affected individuals with a consolidated report containing information from the three major credit bureaus. Third, we will be providing credit monitoring service for one year. Fourth, for those individuals who do become victims of fraud, we will provide them with ID theft counselors to help them through the process of clearing their credit reports of any information from related fraudulent activity.

Because this is an ongoing law enforcement investigation, the U.S. Secret Service has advised us that discussing additional details could compromise its investigation.

THE TYPES OF MEASURES USED TO SAFEGUARD IDENTIFIABLE INFORMATION

LexisNexis has long recognized the importance of undertaking extensive measures to protect the information in our databases and has in place a comprehensive security program. Maintaining security is a not a static process, but rather involves continuously evaluating and adjusting our security program in light of technological advances and perceived or real threats.

LexisNexis has physical, administrative, and technical measures to protect the security of information it maintains on its services. Our data facilities are physically secure. Comprehensive monitoring capabilities exist throughout these facilities. These capabilities include interior and exterior cameras and a badge-access system with badge readers at all key entry points in the building, which are monitored 24x7 by on-site security guards.

Administratively, we limit access to data center facilities to those individuals with job-related needs and management authorization. To prevent employee misuse of our systems, we have policies and procedures in place to monitor usage and address policy abuses through clearly stated measures, up to and including termination.

In addition, we limit a customer's access to information, including sensitive information, in LexisNexis products according to the purposes for which they seek to use the information. Our Chief Privacy Officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong privacy policies in place to help

protect the privacy of information contained in our databases. We also undertake regular assessments by independent third parties of both our privacy and security practices. In addition, because we recognize that the success of our security program depends on our employees, we have developed training programs on privacy and security policies and practices.

We use a multi-layered technical approach to securing data and applications. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities.

In addition to the security safeguards outlined above, LexisNexis has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information contained in our systems. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials. We also authenticate the documents provided to us to ensure they have not been tampered with or forged.

We have verification procedures in place to vet customers prior to providing them with access to sensitive information. Customers requesting access to sensitive information must go through a multi-step application and approval process. Only those customers with a permissible purpose under federal law are granted access to sensitive data such as driver's license information and social security numbers. In addition, customers are required to make express representations and warranties regarding access and use of sensitive information.

LexisNexis plans to further restrict access to the most sensitive data elements, Social Security Numbers and Driver's License Numbers, by extending LexisNexis current more restrictive SSN truncation policy to its recently acquired Seisint business and is adding a policy to include the masking of DLNs. These steps are part of the on-going review that LexisNexis has been conducting on security practices, authorization and verification procedures and privacy policies across its businesses.

We have also accelerated our program to review and integrate verification and security procedures at LexisNexis and Seisint. Specifically, LexisNexis is in the process of:

- Enhancing ID and password administration procedures;
- Enhancing security requirements applied to our customers; and
- Working with law enforcement and outside consultants to establish new procedures and techniques to thwart criminal activity.

THE TYPES OF INFORMATION MAINTAINED BY LEXISNEXIS

The information maintained by LexisNexis falls into the following three general classifications: public record information, publicly available information, and non-public information. I briefly describe each below.

Public record information. Public record information is information originally obtained from government records that are available to the public. Land records, court records, and professional licensing records are examples of public record information collected and maintained by the government for public purposes, including dissemination to the public.

Publicly available information. Publicly available information is information about an individual that is available to the general public from non-governmental sources. Some examples of these non-governmental sources are telephone directories, newspaper reports, and other general-distribution publications.

Non-public information. Non-public information is information about an individual that is not obtained directly from public record information or publicly available information. This information comes from proprietary or non-public sources. Non-public data maintained by LexisNexis consists primarily of information obtained from either motor vehicle records or so-called credit header data. Credit header data is the non-financial individual identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, social security number, and month and year of birth.

LAWS GOVERNING LEXISNEXIS COMPILATION AND DISSEMINATION OF IDENTIFIABLE INFORMATION

There are a wide range of federal and state privacy laws to which LexisNexis is subject in the collection and distribution of personally identifiable information. These include:

The Gramm-Leach-Bliley Act. Social security numbers are one of the two most sensitive types of information that we maintain in our systems and credit headers are the principal commercial source of social security numbers. Credit header data

is obtained from consumer reporting agencies.[1] Starting in July 2001, the compilation of credit header data is subject to the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§6801 *et seq.,* and information subject to the GLBA cannot be distributed except for purposes specified by the Congress, such as the prevention of fraud. For credit header data compiled prior to July 2001, the dissemination of this information is subject to a set of industry-developed principles endorsed and enforced by the Federal Trade Commission.

Driver's Privacy Protection Act. The compilation and distribution of driver's license numbers and other information obtained from driver's licenses are subject to the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. §§2721 *et seq.,* as well as state laws. Information subject to the DPPA cannot be distributed except for purposes specified by the Congress, such as fraud prevention, insurance claim investigation, and the execution of judgments.

Telecommunications Act of 1996. Telephone directories and similar publicly available repositories are a major source of name, address, and telephone number information. The dissemination of telephone directory and directory assistance information is subject to the requirements of the Telecommunications Act of 1996, as well as state law.

FOIA and other Open Records Laws: Records held by local, state, and federal governments are another major source of name, address, and other personally identifiable information. The Freedom of Information Act, state open record laws, and judicial rules govern the ability of LexisNexis to access and distribute personally identifiable information obtained from government agencies and entities. *See, e.g.,* 5 U.S.C. § 552.

Other laws:

Unfair and Deceptive Practice Laws: Section 5 of the Federal Trade Commission Act, and its state counterparts, prohibit companies from making deceptive claims about their privacy and security practices. These laws have served as the basis for enforcement actions by the Federal Trade Commission and state attorneys general for inadequate information security practices. The consent orders settling these enforcement actions typically have required companies to implement information security programs that conform to the standards set forth in the GLBA Safeguards Rule, 16 C.F.R. Part 314.

Information Security Laws: A growing body of state law imposes obligations upon information service providers to safeguard the identifiable information they maintain. For example, California has enacted two statutes that require businesses to implement and maintain reasonable security practices and procedures and, in the event of a security breach, to notify individuals whose personal information has been compromised. See California Civil Code §§1798.81.5, 1798.82-84.

LEGISLATIVE MEASURES LEXISNEXIS SUPPORTS

We recognize that additional legislation may be necessary to address the growing problem of cybercrime and identity theft. LexisNexis supports the following legislative approaches:

Data Security Breach Notification. Consistent with the proposals outlined by FTC Chairman Majoras in her testimony before the Senate Banking Committee last week, we support requiring notification in the event of a security breach where there is substantial risk of harm to consumers. We share the concerns that Chairman Majoras raised in her testimony about ensuring that there is an appropriate threshold for when customers actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that it is important that any such proposal contain federal preemption to insure that companies can quickly and effectively notify consumers and not struggle with complying with multiple, potentially conflicting and inconsistent state laws.

Adoption of Data Security Safeguards for Information Service Providers Modeled After the GLBA Safeguard Rule. LexisNexis would support the proposal outlined by Chairman Majoras whereby the types of security protections required by the Safeguard Rule of the GLBA would be applicable to information service providers that are not themselves "financial institutions" as defined under GLBA.

Increased penalties for identity theft and other cybercrimes and increased resources for law enforcement. LexisNexis strongly encourages legislation that imposes more stringent penalties for identity theft and other cybercrimes. Additionally, consumers

[1] Consumer reporting agencies are governed by the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§1681 *et seq.* Some information services, such as Seisint's Securint service and LexisNexis PeopleWise, also are subject to the requirements of the FCRA.

and industry alike would benefit from enhanced training for law enforcement and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and cybercrime. Too many of our law enforcement agencies do not have the resources to neutralize these high-tech criminals.

It is critical that any legislation being considered ensure that legitimate businesses, government agencies, and other organizations continue to have access to identifying information that they depend on for important purposes including fraud detection and prevention, law enforcement, and other critical applications. Moreover, legislation must strike the right balance between protecting privacy and ensuring continued access to critically important information that is provided through information service providers.

CONCLUSION

Mr. Chairman, members of the Subcommittee, thank you again for the opportunity to testify before you today. LexisNexis is committed to:

- Developing effective products involving the responsible use of personally identifiable information to support law enforcement, government, and responsible businesses ;
- Safeguarding consumer privacy; and
- Protecting the security of our data systems.

We look forward to working with you as you develop proposals to help protect consumers and help fight cybercrime and identity theft.

Mr. STEARNS. Thank you, Mr. Sanford. I was hoping we could get the second opening statement in. We have one vote, and then no votes for a long period of time.

So Mr. Smith, we are going to have to recess the subcommittee, and I will go vote, and members have just been emailed to come back, so the subcommittee is——

[Brief recess.]

Mr. STEARNS. [continuing] members will be filing in, but Mr. Smith, we wanted to give you an opportunity to proceed.

Mr. SMITH. Chairman——

Mr. STEARNS. And just move it a little closer. Sometimes, it is—if you don't mind, that would be helpful. Thanks.

STATEMENT OF DEREK SMITH

Mr. SMITH. Chairman Stearns, Representative Schakowsky, and members of the committee. I am Derek Smith, Chairman and Chief Executive Officer of ChoicePoint, Inc.

I have thought a great deal, both professionally and as a father, about the role information can play in making our world more or less secure. I have devoted the last 12 years to the pursuit of making our society safer through the innovative but proper use of information and technology.

At ChoicePoint, our customers cover a broad spectrum of American business, nonprofits, and government services organizations, including most of America's Federal, State, and local law enforcement agencies. Last year, ChoicePoint helped 100 million American consumers obtain fairly priced home and auto insurance, and thousands of American businesses obtain commercial property insurance.

We also helped 8 million Americans get jobs through our workplace pre-employment screening services. We helped more than 1 million consumers obtain expedited copies of their vital records, birth, death, and marriage certificates. ChoicePoint helped government fulfill its mission guarding the safety of Americans.

But regrettably, I know that I am not here today to talk only about the good things that ChoicePoint has done. I know I am here

because your committee and your constituents are concerned about the harm that may have been done to approximately 145,000 Americans whose information may have fallen into the hands of criminals who accessed ChoicePoint systems.

Let me begin by offering an apology on behalf of our company, and my own personal apology to those consumers whose information may have been accessed by the criminals whose fraudulent activity ChoicePoint failed to prevent. Beyond our apology, I want to assure the public and the members of this committee that we have moved aggressively to safeguard the information in our possession from future criminal theft.

We have also moved promptly to provide assistance to every affected individual, to help them avoid financial harm. We are also participating in the efforts of—we also welcome participating in the efforts of this committee and other policymakers seeking to provide an appropriate regulation of our industry. We have decided to exit the consumer-sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will no longer sell information products containing sensitive consumer data, including Social Security and driver's license numbers, except where there is a specific consumer-driven transaction or benefit, or where the products support Federal, State, or local government and criminal justice purposes.

ChoicePoint will continue to provide authentication, fraud prevention, and other services to large, accredited customers, where consumers have existing relationships. We have strengthened ChoicePoint's customer credentialing process, and we are changing our products and services to many customer segments. We are requiring additional due diligence, such as bank references and site visits, to small business applications before allowing access to personally identifiable information.

We are recredentialing broad sections of our customer base, including our small business customers. We are modifying the services that ChoicePoint is delivering to our customers. I have created an Office of Credentialing Compliance and Privacy that will report to our Board of Directors Privacy Committee, and be independent of ChoicePoint management. This Office will be led by Carol DiBattiste, previously Deputy Administrator of the Transportation Security Administration, and a former senior prosecutor in the Department of Justice, with extensive experience in detection and prosecution of financial fraud.

I have also appointed Robert McConnell, a 28 year veteran of the Secret Service and former chief of the Federal Government's Nigerian Organized Crime Taskforce, to serve as our liaison to law enforcement officials. These changes reflect some of the lessons that we have already learned as a result of the breaches of ChoicePoint security, which have resulted in the recent convictions of several individuals.

From what I now know, on September 27, 2004, a ChoicePoint employee became suspicious while credentialing a prospective small business customer based in the Los Angeles area. This employee brought his concerns regarding the application to our Security Services Department. After a preliminary review, the manager of the Security Services Department alerted the Los Angeles County

Sheriff's Department. They decided to initiate an official police investigation, and asked for our assistance. The investigation is still ongoing, and has, I am told, already resulted in the arrest and conviction of at least one individual.

After the situation became public last month, I learned that another instance in which ChoicePoint had been working with law enforcement inquiry also involved a criminal use of our information products, and late last year, had resulted in a guilty plea.

With respect to California, we have learned that those involved had previously opened ChoicePoint accounts by presenting fraudulently obtained California business licenses and other fraudulent documents. They were able to access information products primarily containing the following information: consumer names, current and former addresses, Social Security numbers, driver's license numbers, certain other public record information such as bankruptcies, liens, and judgments, and, in certain cases, credit reports.

Based on the information currently available, we estimate the data from approximately 145,000 consumers may have been accessed as a result of unauthorized access to our information products. Nearly one quarter of those consumers are California residents. California is the only State that statutorily requires affected consumers to be notified of a potential breach of personally identifiable information, and authorized law enforcement officials to delay notification to allow a criminal investigation to proceed.

Last fall, ChoicePoint received such a request from the Sheriff's Department, after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time, ChoicePoint had not yet reconstructed all the searches required to identify consumers at risk, and law enforcement officers had not yet learned all the pertinent details of the crime. Working cooperatively with the Sheriff's Department, and after completing the necessary reconstruction, we began the process of notifying consumers last month. We voluntarily elected to use the California law as the basis for notifying consumers in all States.

Absent specific notification from law enforcement personnel, affected consumers, or others, we cannot determine whether a particular consumer has been a victim of actual identity theft. However, law enforcement officials have informed us that they have identified approximately 750 consumers nationwide, where some attempt was made to compromise their identity. The security breach that ChoicePoint discovered last fall in California has caused us to go through some serious soul searching at ChoicePoint.

In retrospect, the company should have acted more quickly. I should have been notified earlier of the investigation being conducted by the Los Angeles County Sheriff's Department. What I can tell you today is that from now on, I will be notified when ChoicePoint learns of a formal law enforcement inquiry involving any potential breach of our security.

In the meantime, we have taken other steps to help and protect the consumers who may have been harmed. First, ChoicePoint established a dedicated toll-free customer service number, and a special website to respond to inquiries. Second, we are providing, free

of charge, a combined three bureau credit report. Third, we are providing, free of charge, a 1-year credit monitoring service, and for anyone who has suffered actual identity theft from this fraud, ChoicePoint will provide further assistance to help them resolve any issue arising from that identity theft. We hope these efforts will help those individuals protect their personal data from being used in a criminal manner, and that they will mitigate any harm.

Mr. Chairman, to conclude, I would like to state before this committee, for the record, my position on further regulation or oversight of information and credential verification providers. For the past 2 years, I have been working to prompt a broad discussion on how we can build a framework that defines how personally identifiable information should be used, by whom, and for what purpose.

I have called for independent oversight to give the public the confidence it needs. I support increased penalties, criminal penalties, for the unauthorized access to information. I support a single, reasonable, nationwide, mandatory notification requirement of any unauthorized access to personally identifiable information.

Every advance in technology that makes our lives easier also makes it easier for enemies to move swiftly against us. You and I can be approved for a bank account in a matter of minutes, but a person can use that same technology to get a false or real driver's license, or to create a fake business. The point being, technology and information are neither good nor bad. People determine if the power of information is used for the benefit of individuals or society, or to create harm.

I believe that only by adding a more formal structure to the current scheme of information use will we realize the full value of technology-based tools to society. The architects of these guidelines will be working against a backdrop of apparently conflicting principles. Increased concerns about privacy, balanced against society's need to identify people who would do us harm. But it is important to remember that these two principles are not mutually exclusive, and that too much weight on either end of the spectrum leads not to balance, but to immobility, or worse, to a breaking point.

The privacy debate should not be a choice between civil defense and civil liberty. We must aim to preserve both. We look forward to participating in the continued discussion of these issues, and I pledge our cooperation and my personal cooperation to these efforts.

I thank you for your consideration, and I will be pleased to answer any questions you might have.

[The prepared statement of Derek Smith follows:]

PREPARED STATEMENT OF DEREK SMITH, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CHOICEPOINT INC.

Chairman Stearns, Representative Schakowsky, and Members of the Committee: I am Derek Smith, Chairman and Chief Executive Officer of ChoicePoint Inc.

I have thought a great deal, both professionally and as a father, about the role information can play in making our world more, or less, secure. I have devoted the last 12 years to the pursuit of making our society safer through the innovative, but proper, use of technology and information.

At ChoicePoint, our customers cover a broad spectrum of American business, nonprofits and government service organizations—from half the Fortune 1000 to notable community organizations, and most of America's federal, state and local law enforcement agencies.

Last year ChoicePoint helped 100 million American consumers obtain fairly priced home and auto insurance, and thousands of American businesses obtain commercial property insurance. We also helped 8 million Americans get jobs through our workplace pre-employment screening services. We helped more than one million consumers obtain expedited copies of their vital records—birth, death and marriage certificates. ChoicePoint helped government fulfill its mission guarding the safety of Americans.

But regretfully, I know that I am not here today to talk only about the good things ChoicePoint has done. I know I am here because your committee and your constituents are concerned about the harm that may have been done to approximately 145,000 Americans, whose information may have fallen into the hands of criminals who accessed ChoicePoint systems.

Let me begin by offering an apology on behalf of our company, as well as my own personal apology, to those consumers whose information may have been accessed by the criminals whose fraudulent activity ChoicePoint failed to prevent.

Beyond our apology, I want to assure the public and the members of this committee that we have moved aggressively to safeguard the information in our possession from future criminal theft. We have also moved promptly to provide assistance to every affected individual to help them avoid financial harm. We also welcome participating in the efforts of this Committee and other policy-makers seeking to provide an appropriate regulation of our industry.

We have decided to exit the consumer sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will no longer sell information products containing sensitive consumer data including social security and drivers license numbers except where there is a specific consumer driven transaction or benefit or where the products support federal, state or local government and criminal justice purposes. ChoicePoint will continue to provide authentication, fraud prevention and other services to large accredited corporate customers where consumers have existing relationships.

We have strengthened ChoicePoint's customer credentialing process and we are changing our products and services to many customer segments. We are requiring additional due diligence such as bank references and site visits to small business applicants before allowing access to personally identifiable information. We are recredentialing broad sections of our customer base, including our small business customers. We are modifying the services that ChoicePoint is delivering to our customers.

The remaining ChoicePoint products and services that contain sensitive information will satisfy one of three tests:

- Support consumer driven transactions, for which data is needed to complete or maintain relationships such as insurance, employment or tenant screening.
- Provide authentication or fraud prevention tools to large, accredited corporate customers to enable services such as identity verification, customer enrollment or insurance claims.
- Support federal, state or local government and law enforcement purposes.

I have created an office of Credentialing, Compliance and Privacy that will report to our Board of Directors' Privacy Committee and be independent of ChoicePoint management. This office will be based here in Washington and be led by Carol DiBattiste, previously deputy administrator of the Transportation Security Administration and a former senior prosecutor in the Department of Justice with extensive experience in the detection and prosecution of financial fraud.

I have also appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the federal government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials.

These changes reflect some of the lessons we have already learned as a result of the breaches of ChoicePoint's security which have resulted in the recent convictions of several individuals.

From what I now know, on September 27, 2004 a ChoicePoint employee became suspicious while credentialing a prospective small business customer based in the Los Angeles area. This employee brought his concerns regarding the application to our Security Services Department. After a preliminary review, the manager of the Security Services Department alerted the Los Angeles County Sheriff's Department. They decided to initiate an official police investigation and asked for our assistance. That investigation is still ongoing, and has, I am told, already resulted in the arrest and conviction of at least one individual.

After this situation became public last month I learned that another instance in which ChoicePoint had been working with a law enforcement inquiry also involved a criminal use of our information products and, late last year, had resulted in a guilty plea.

With respect to California, we have learned that those involved had previously opened ChoicePoint accounts by presenting fraudulently obtained California business licenses and fraudulent documents. They were then able to access information products primarily containing the following information: consumer names, current and former addresses, social security numbers, driver's license numbers, certain other public record information such as bankruptcies, liens and judgments and, in certain cases, credit reports.

Based on information currently available, we estimate that data from approximately 145,000 consumers may have been accessed as a result of unauthorized access to our information products. Nearly one quarter of those consumers are California residents. California is the only state that statutorily requires affected consumers to be notified of a potential breach of personally identifiable information, and authorizes law enforcement officials to delay notification to allow a criminal investigation to proceed. Last fall, ChoicePoint received such a request from the Sheriff's Department after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time ChoicePoint had not yet reconstructed all of the searches required to identify consumers at risk and law enforcement officers had not yet learned all of the pertinent details of the crime. Working cooperatively with the Sheriff's Department and after completing the necessary reconstruction, we began the process of notifying consumers last month. We voluntarily elected to use the California law as the basis for notifying consumers in all states. Absent specific notification from law enforcement personnel, affected consumers or others, we can not determine whether a particular consumer has been a victim of actual identity theft. However, law enforcement officials have informed us that they have identified approximately 750 consumers nationwide where some attempt was made to compromise their identity.

The security breach that ChoicePoint discovered last fall in California has caused us to go through some serious soul-searching at ChoicePoint. In retrospect, the company should have acted more quickly. I should have been notified earlier of the investigation being conducted by Los Angeles County Sheriff's Department. What I can tell you today is that from now on, I will be notified when ChoicePoint learns of a formal law enforcement inquiry involving any potential breach of our security.

In the meantime, we have taken other steps to help and protect the consumers who may have been harmed.

- First, ChoicePoint has established a dedicated toll-free customer service number and a special web site to respond to inquiries;
- Second, we are providing, free of charge, a combined three-bureau credit report;
- Third, we are providing, free of charge, a one-year credit monitoring service; and
- For anyone who has suffered actual identity theft from this fraud, ChoicePoint will provide further assistance to help them resolve any issue arising from that identity theft.

We hope these efforts will help those individuals protect their personal data from being used in a criminal manner and that they will mitigate any harm.

Mr. Chairman, I would like to state before this committee, for the record, my position on further regulation or oversight of information and credential verification providers. For the past two years, I have been working to prompt a broad discussion on how we can build a framework that defines how personally identifiable information should be used, by whom and for what purposes. I have called for independent oversight to give the public the confidence it needs. I support increased penalties—criminal penalties—for the unauthorized access to information. I support a single, reasonable, nationwide mandatory notification requirement of any unauthorized access to personally identifiable information.

Every advance in technology that makes our lives easier also makes it easier for our enemies to move swiftly against us. You and I can be approved for a bank account in a matter of minutes, but a person can use that same technology to get a fake or real drivers' license or to create a fake business.

The point being, technology and information are neither good nor bad. People determine if the power of information is used for the benefit of individuals or society or to create harm.

I believe that only by adding a more formal structure to the current scheme of information use, will we realize the full value of technology-based tools to society.

The architects of these guidelines will be working against a backdrop of apparently conflicting principles: increased concerns about privacy balanced against society's need to identify people who would do us harm. But it is important to remember that these two principles are not mutually exclusive, and that too much weight on either end of the spectrum leads not to balance, but to immobility, or worse, to a

breaking point. The privacy debate should not be a choice between civil defense and civil liberty. We must aim to preserve both.

Perhaps I might take a few minutes to describe some of the benefits of having access to an individual's personal information. ChoicePoint has helped find more than 800 missing children—we were even able to find a baby kidnapped from a hospital the day he was born, and return him to his parents within 24 hours. Our company works with the largest youth services organizations around the country to help them screen volunteers—we have helped identify more than 11,000 undisclosed felons among those volunteering, or seeking to volunteer. Included in this group, individuals who did not disclose they had been convicted of a collective 5176 violent crimes, 1137 sex crimes, 11,397 illegal substance offenses, 1055 crimes against children. Forty-two of these individuals were registered sex offenders.

ChoicePoint's DNA laboratories have freed those wrongly accused from prison, and helped to identify suspects and victims of violent crimes. Our labs matched thousands of bone fragments found in the World Trade Center rubble with DNA samples provided by victims' families. Our scientists are currently in the tsunami ravaged areas of Asia helping to identify victims to help bring closure to families devastated by the disaster.

ChoicePoint helped Maryland police identify and locate two men named John Allen Muhammad and Lee Boyd Malvo. The two had no obvious relationship to one another and no known ties to Washington, DC. Information technology found those hidden links, and provided the tools for locating the people now known as the DC Snipers.

In fact, ChoicePoint provides service to more than 7,000 federal, state and local law enforcement agencies.

Not all of what we do is so dramatic. ChoicePoint also serves 700 insurance companies, a large number of Fortune 500 companies, and many large financial services companies.

And the products involved in these transactions are regulated by the FCRA, which represents a significant portion of our business. Certain other segments of our business are regulated by Gramm-Leach-Bliley Act and various state laws.

We look forward to participating in continued discussion of these issues, and I pledge our cooperation to your efforts.

I thank you for your consideration, and I would be pleased to answer any questions you might have.

Mr. STEARNS. I thank you, Mr. Smith, and first of all, I would like to thank both of you, a President and CEO, Mr. Sanford, and a Chairman and CEO, Mr. Smith, for coming here to speak about these important issues.

And I would caution all members that they cannot actually talk about the investigation with the Federal investigation going on. It is going to be difficult for them to talk about it, but they obviously can talk about what happened, and give us policy presentation on what they think should happen.

Mr. Smith, my first question is to you. And I—you know, everything I have read about this report in the paper. We have had a little conversation ourselves. This case, a man from Los Angeles filled out all the proper applications to receive information from ChoicePoint, and it appears that due diligence by you was to confirm his application, confirm a copy of a business license he had. Evidently, this person paid his bills, received information, including consumers' Social Security numbers, which the person used fraudulently.

So the question for you is, based upon that scenario, what would you do differently knowing what you do today, to make sure that this person who got this business license, who paid his bills, that seemed to be, to you, a legitimate customer, how would you have stopped that, today?

Mr. SMITH. Well, I think that there are a couple things. First, we are strengthening the credentialing procedures now to include even a more rigorous analysis of that process——

Mr. STEARNS. Can you strengthen it——

Mr. SMITH. [continuing] to include——

Mr. STEARNS. [continuing] good enough, you think? On your own, do you think you can strengthen it good enough?

Mr. SMITH. Well, the reality is, one of the reasons why we are exiting the consumer-sensitive market, particularly as it relates to small businesses, is that it is possible for a business to set up themselves as a legitimate business, operate as a legitimate business, and yet, then subsequently use that particular business for access to information that would be inappropriate.

We can't find out how we would avoid that, and as we went back through our recredentialing procedures, we determined that the only way in which we could prevent the data from being accessed inappropriately in that circumstance, was in fact, to restrict the data and not provide it all in those instances, or in a masked format.

Mr. STEARNS. Well, that is what it seems to me. Now, as I understand, I read that a scam like this had been perpetrated against ChoicePoint before. Is that correct?

Mr. SMITH. Well, what had happened is, back in 2001, we had received a subpoena about one particular account. During 2002, we actually received three subpoenas asking for additional information about that account, but then, we never heard anything else for almost a 2½ year period of time. And then, in late 2004, we were asked to testify, potentially, at a trial of an individual, which is the first time we had heard about that since that point in time, that the person subsequently pleaded guilty, and we were not asked to testify. So during that previous incident, we had had subpoenas, but we had not understood what the nature of the investigation was, or what potentially the crime was, until just recently.

Mr. STEARNS. Is there any way for a private citizen to find out what types of information ChoicePoint data base may contain about him or her?

Mr. SMITH. There are several. I mean, to the extent that a majority of products are actually governed under the Fair Credit Reporting Act, and you have the right to be able to get a copy of those particular reports. In the public record arena, we do provide individuals who request access to those reports a copy of a specific report, as it references themselves.

Mr. STEARNS. Mr. Stanford, now your case is a little differently than ChoicePoint. A person stole sensitive information about consumers by the use of passwords fraudulently obtained from your customer. And I guess the customers affected the breach—do the customers affected by the breach have to worry about identity theft for the rest of their lives, and when will the elevated risk of identity theft subside, if ever?

Mr. SANFORD. Well, sir, in our situation, the facts as we understand them, and I think we talked about this yesterday, in early February of this year, one of our integration teams, recall that we acquired the Seisint business late in 2004, one of our integration teams which was charged with the responsibility of reviewing the security procedures, authentication, verification, and kind of the physical security of the business we acquired. It came to their attention that there were some irregular billing activities in a hand-

ful of accounts, and they did that investigation. They gathered more facts, they brought that to my attention late in February, I think it was the February 28, and on March 2, I got on an airplane and flew here to Washington, DC., and met with the Assistant Director of the United States Secret Service, and asked them if they would investigate it for us, and we have turned over our records.

We don't know yet how that compromise occurred in the customer environment. Law enforcement is investigating that, and we will be forthright and share the details of that investigation when it is completed.

Mr. STEARNS. I am sorry I am asking you to speculate. It is probably not fair, but you know, this identity theft, what is your experience about—does it last a year, or 2 years? I mean, what—I mean, this is—I mean, I've run into people that say it is a long time.

Mr. SANFORD. I haven't seen any statistics that indicate a time, you know, a cause and effect timeline that says, if an identity, you know, if a record is, you know, obtained fraudulently, you know, is that going to then be used 4 or 5 years later? I don't know——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] if there are any published reports on that, sir.

Mr. STEARNS. Now, in your case, it wasn't LexisNexis. It was Seisint. And this company, you acquired. And is it possible that Seisint outsourced, in other words, they are a subcontractor, they have this information, you are the parent—they are not a subcontractor, but they are owned by you. But is your data base effectively outsourced to all your customers, so that a breach of their security systems potentially allows criminals access to sensitive information in your data bases?

Mr. SANFORD. I am not sure I understand the question. Let me see if I can respond, and let me know if I am responsive to what you are looking for. This is our company. We bought this company.

Mr. STEARNS. Right.

Mr. SANFORD. This is not a subcontractor.

Mr. STEARNS. Right.

Mr. SANFORD. This is a LexisNexis business——

Mr. STEARNS. Yeah.

Mr. SANFORD. [continuing] that was acquired in the second half of 2004. We enter into agreements with legitimate businesses who subscribe to services. They have password and ID access to a data base that we maintain.

Mr. STEARNS. Does Seisint outsource some of their business to some other companies?

Mr. SANFORD. We license some of our data base information to——

Mr. STEARNS. Okay. So my question is, when you license it to these other companies, is it possible their employees, then, would have access to this information, they could fraudulently do it?

Mr. SANFORD. I am still not sure I follow the question, sir.

Mr. STEARNS. Okay. So if your new company outsources a lot of their work, they give them the identity of individuals to process, and——

Mr. SANFORD. We license our data to other parties who are resellers, credit bureaus, for example.

Mr. STEARNS. Okay.

Mr. SANFORD. And they contractually enter into agreements with us to comply with all the same safety, verification, security safeguards that we have in place for our business.

Mr. STEARNS. So I think what we are saying is, if you allow employees to have access to this information through passwords, then you are effectively outsourcing the ability of others to get access to this secured information.

Mr. SANFORD. I am—I don't—I still don't understand how I am outsourcing to employees.

Mr. STEARNS. Okay. Okay. My time has expired. The Ranking woman, Ms. Schakowsky.

Ms. SCHAKOWSKY. Okay. First, Mr. Smith, in your SEC filing about the 145,000 consumers that were exposed, you say that that number represents those whose data was compromised after July 1, 2003, when the California law required you to report.

We know that there were earlier breaches, in fact, prior to 2003, that you were unaware of, the Benson case, where they pled guilty and were guilty of fraud. So I would assume, then, the numbers are higher than 145,000. Do you have any idea what that number is, and are you going back at all to review your records to find out if there were earlier breaches? What is your plan here?

Mr. SMITH. The Board or the committee has sanctioned a study to go back and to look at not only this incident, but prior incidents, to determine if, in fact, any other such circumstances took place. And so that investigation is currently underway, and is being done on a very aggressive basis.

Ms. SCHAKOWSKY. I have to say that I am pretty surprised, and I think a number of other people were, would be as well, to find out that there was this case, you said subpoenas were issued, but I guess you didn't bother to figure out why or what the case was about, that you would have been unaware of a criminal prosecution that resulted in a conviction. How could that happen, and has anybody been made to take responsibility for that at all?

Mr. SMITH. Well, we do receive subpoenas to support law enforcement investigations. They don't always give us information, because of the sensitive nature of the investigation, what type of investigation it might be. It could have been involved in a situation such as identity theft, but it could have been involved in any other type of criminal potential incident.

Ms. SCHAKOWSKY. So in other words, such an instance could go unnoticed still?

Mr. SMITH. No, not today, as I have said, that we have now changed our procedures so that in any circumstance where we are issued a subpoena, it will be elevated to me personally. We have also instituted a new department that is in charge of all of our credentialing compliance and privacy. It is headed up by Carol DiBattiste, who is a recognized leader in this area, and she will be assuring that any type situation that this occurs in the future will be dealt with very quickly, and will be elevated appropriately and responsibly——

Ms. SCHAKOWSKY. Okay.

Mr. SMITH. [continuing] immediately.

Ms. SCHAKOWSKY. You know, you said that some information is available to the public if they ask for it. People understand about credit reporting agencies, but I have a feeling before all this came out with LexisNexis and with ChoicePoint that nobody even knew really, hardly anybody knew about you. Could you provide us with information, or—unless you have it at your fingertips, of how many people have actually asked for their information from you before the ChoicePoint, before these scandals were revealed?

Mr. SMITH. I will have to get you, and will be pleased to get you that particular information.

Ms. SCHAKOWSKY. Do you have any order of magnitude, of how many people actually asked for that information?

Mr. SMITH. Again, many of our products and services are under the Fair Credit Reporting Act, so that they would naturally be part of the new FACT act, which requires a free copy of that report——

Ms. SCHAKOWSKY. I understand what the requirement is, but I am saying I don't think there is a lot of consumer awareness about it, and I am just wondering——

Mr. SMITH. There has not been——

Ms. SCHAKOWSKY. [continuing] how many people——

Mr. SMITH. [continuing] an overwhelming number of people who have requested the reports. That would be correct.

Ms. SCHAKOWSKY. Thousands of voters were inaccurately listed as felons by your company in 2000, and were denied the right to vote in the Florida election. That is very serious, and we are talking more about identity theft, et cetera, but this precious right to vote. Were any laws violated by that?

Mr. SMITH. Well, first, I appreciate the opportunity to respond to that particular question and situation. The incident you are referring to was a project done between a company called Data base Technologies and the State of Florida. It was operated and run between 1998 and roughly 2000. At that particular point in time, Data base Technologies was a very significant competitor to ChoicePoint.

In the middle of 2000, but prior to the election, but after all of that information had been provided to the State of Florida, we acquired that company. So ChoicePoint was not involved in any way in screening the voter rolls, in dealing with the issues of what potential people were allowed to vote. We have not been involved in any such situation in that regard. So unfortunately, because we acquired that company, it has been interpreted that we were involved. But we were not involved at all in that particular situation.

Ms. SCHAKOWSKY. Did you know about it when you acquired them?

Mr. SMITH. We—I—we did not. It was a contract between themselves and the State of Florida.

Ms. SCHAKOWSKY. If I could ask this last question, I realize it may go over time, but I want to know from both of you, what quality assessment of your data do you do? How do you ensure that the information on people is correct, and perhaps, most importantly, what do you feel is your responsibility if someone is denied a home or a job or insurance because the information you are selling and profiting from about them is wrong?

Mr. Sanford.

Mr. SANFORD. Sure. Congresswoman, we have a very few products that are governed by the FCRA. These are products that are involved in employment screening. And we follow a rigorous procedure to make corrections. I personally get emails from time to time, even phone calls from consumers that want to question the accuracy of data in our data bases. We have a group of lawyers who work with them. They have to first go through an authentication and verification procedure to make sure they really are who they say purport to be, and then, we work with them to make corrections in the data base. Sometimes, that requires them to go back to the source of where we got that data from. Perhaps there is an error in a credit header that we got from a credit bureau. The overwhelming majority of——

Ms. SCHAKOWSKY. So they have to go back. You don't have to go back. They have to go back.

Mr. SANFORD. Well, normally, a credit bureau would not allow us to correct a record of a consumer, since we are not that consumer. We wouldn't have the legal authority to do that.

Ms. SCHAKOWSKY. Well, it is a source of data that you got it from, though.

Mr. SANFORD. We help them. We, you know, we advise them of how they can make that correction. With respect to the rest of the data in our systems, it is principally public record information. And public record information is just that, information that we get from public sources.

And again, we don't have the authority to change an official public record that we have in our data base. We tell people who ask these questions where we got the data from, where the source is, to the extent that we have the contact information, we provide them with that, and we ask them to go and correct that. As soon as that is corrected, our records are updated, and then, we have inaccurate information in our systems.

Mr. SMITH. Again, we apply extraordinarily rigorous standards to ensure the accuracy of the information. And I would suggest that—I believe that people should have the right to access their public records, and that if, in fact, they should have the right to question the accuracy of that information, and have it done in a very prompt way.

Again, there are cases where, when that information is inaccurate, the important part is to direct them back immediately to the source of that information, which many times, is in some kind of State repository. Otherwise, even if we had the ability to change the information, it would perpetuate itself through the system, because the source document itself was fundamentally wrong.

I do believe that we should allow consumers, though, to have, much like it is in a credit report, the ability to make a comment on their public record, if a record is deemed correct, but they want to make a comment, because there is some extenuating circumstance associated with that information, they should have the ability to do so, and I support that.

Mr. STEARNS. The gentlelady's time has expired. The gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman. A couple of brief questions. Mr. Smith, you anticipated one of my questions in your testi-

mony, when you expressed support for mandatory disclosure of any sort of security breach in which consumers' data is compromised.

I didn't hear, Mr. Sanford, did you take such a position, and is that your position also?

Mr. SANFORD. Yes, we thought that the approach that the Chairwoman of the Federal Trade Commission has outlined in her testimony not only here today, but last week, in the Senate Banking Committee, is a very sensible approach.

I can tell you that we, as a matter of policy, are notifying consumers, where we believe there is a significant risk that some harm could come to those consumers, irrespective of the State in which that consumer resides.

I am very concerned that if we do have a host of notification bills enacted across the United States in 30, 40, 50 jurisdictions, that we will actually defeat the intent of what those statutes were intended to do, which is to put consumers on notice, and have them take appropriate actions.

If they get flooded with a whole variety of different standards, different bills, different approaches, I think we are going to confuse consumers, and defeat the purpose of what the legislation would have been intended from the first place.

So a national standard, and Federal preemption is most appropriate here. We don't want to flood the market with a bunch of notices, not just from companies like information services, but financial institutions, where people lose things. I think if we do that, they are going to end up like the junk mail that people get and go right in the trashcan.

Ms. BALDWIN. Thank you.

Mr. Smith, in your written testimony, and you also reiterated it in your oral testimony, you stated that ChoicePoint would no longer sell information products containing sensitive consumer data, and I quote, "except where there is a specific consumer-driven transaction or benefit."

I am interested in precisely what that means, and particularly, does it mean that a consumer would have to give permission for the release of that specific information, and if not, how do you determine what would benefit the consumer?

Mr. SMITH. Well, to give you an example of a consumer-initiated transaction, it would be things such as the purchase of insurance. It would be seeking employment, potentially, trying to rent an apartment. And so what we were trying to identify there were things that it was in the consumer's best interest, and they, in essence, initiated a transaction.

There may be cases where, and I think, the majority of cases, they would, in fact, have given their consent, but there may be a circumstance where, in seeking a benefit, they didn't directly do that, but in fact, they benefited from that particular process that was taking place, and that certainly can be defined.

Ms. BALDWIN. And how are you defining that?

Mr. SMITH. Well, today, again, we are in the process, over the next 90-day period, as we said, that we were exiting that market. Today, we are not doing it at all. We will try to clarify that to a greater extent as the policy is implemented.

Ms. BALDWIN. Okay. Thank you.

Mr. STEARNS. The gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I apologize, because of the vote schedule, and not being able to question our Chairman of the Federal Trade Commission, but hopefully, we can submit questions.

Mr. STEARNS. Absolutely.

Mr. GREEN. Mr. Derek, Mr. Smith, one, I welcome, and up until I guess 2 months ago, I didn't know what ChoicePoint was, and as a lawyer, I understood what LexisNexis was, over the years, and the expansion. But to find out that not only do you gather this information, but you sell it to folks who want it, I know under current law, I have the right to question the three credit reporting agencies, and to get an annual report. Do any of your companies come under your—come under that requirement?

Mr. SMITH. I will speak first. I mean, over a majority of the products and services that we supply, particularly to the insurance industry, as well as to major employers, who are doing background pre-employment screenings, fall under the jurisdiction of the Fair Credit Reporting Act, and therefore, consumers have the same rights under those applications, as they would any other particular application.

Mr. GREEN. So we would request from ChoicePoint or LexisNexis the information on individual Members of Congress, if we wanted? I mean, I could have my own information, for example. I don't really need it on on the chairman, but the chairman ought to, maybe ought to be interested in what his is in your data base.

Mr. SMITH. You can get information on yourself, yes, sir.

Mr. GREEN. Okay. And I know one of the concerns we have is that the notification, I know California has a notification requirement. Is that notification only when the—what is the requirement under California law for notification?

Mr. SMITH. It is when sensitive personal information may have been compromised.

Mr. GREEN. Okay. So for example, if I applied for a job, and my employer, or potential employer, requested information from you, I would not necessarily know that that is where my potential information was receiving that information from?

Mr. SMITH. No. In fact, that is an application, pre-employment screening, again under the Fair Credit Reporting Act, and they would have to sign an application that allows that that particular background screen to take place. So they would know that the background screening was taking place on behalf of that employer.

Mr. GREEN. Okay. Would they know it would be ChoicePoint or LexisNexis? Or would it just be—it is a general approval that I say yes, you can do a background check on me?

Mr. SMITH. I don't know whether all specific applications say the company. I would suggest generally that is not true. If you, though, are for some reason denied employment as a result of a particular instance, then that particular company is identified as the company that provided that employer with the specific information.

Mr. GREEN. Again, is that employer required to tell that person——

Mr. SMITH. Yes. Yes, they are.

Mr. GREEN. [continuing] the reasons that—and where the information was from? I guess the MSNBC story worried me a little bit, being from Texas, and when Ms. Pierce's report was, it said "possible Texas criminal history." You know, it seems like that is just a mild innuendo, without saying if you are charged with something, it is public record, and there should be case number or something. Is that typical of what a pre-employment search would say, would be "possible Texas criminal history" without any basis?

Mr. SMITH. No, a typical, in our case, we don't have arrest records that are part of a background pre-employment. These are the actual records that are warehoused by—you actually go into the courthouse, and actually acquire the record itself. So it would be reported as it was in the particular court.

Mr. GREEN. Okay. So you would go to that court, for example, in Harris County, in Houston, Texas, we have the Justice Information Management System, called JIMS. That is public record, and only certain folks, law enforcement, have access to it, typically. And—but you could be able to access that.

Mr. SMITH. I can't speak to the specific instance in which you are talking about, but in general, when a record becomes public in the court itself, then anyone, not just ourselves, would have a right to go——

Mr. GREEN. Okay.

Mr. SMITH. [continuing] and review the record.

Mr. GREEN. Okay. That is true, and I guess what concerns me, instead of saying, you know, I don't know where Ms. Pierce is from, but she said she only visited Texas a few times, what would be the basis for putting in her employment record, "possible Texas criminal history?"

Mr. SMITH. I am not familiar with that. I will certainly be pleased to get back with you at that particular circumstance, but I can't really comment on that incident.

Mr. GREEN. It just seems like in a report, it ought to be more specific, and say, you know, instead of—and this in quotes from the report, "possible Texas criminal history," or "possible New York criminal history." It seemed like it would be—should be more specific. If you are providing that information, and you are responsible, as your company or both your companies, that it would seem like it would be much more specific.

But I am glad to know that I can request my dossier, I haven't done it with the FBI, Mr. Chairman, maybe I ought to do with these two agencies, to see what reports. After my briefcase was stolen last August, I got my reports from Equifax and typically, it was just misnaming, there are a lot Gene Greens that I didn't realize were running around. But anyway, I appreciate that, Mr. Chairman. Thank you.

Mr. STEARNS. I thank the gentleman. The gentleman from Massachusetts.

Mr. MARKEY. Thank you, Mr. Chairman, very much. Mr. Smith, I understand that ChoicePoint is offering consumers who have been victimized by this enormous leakage of personal information a free 1 year credit monitoring service that will enable victims to have access to their credit report, and will provide monitoring and email alerts of changes in consumers' credit report activity.

My concern is what happens after 1 year? My constituents who have written to me, who have been victimized by ChoicePoint's privacy breach, are very concerned about the 1 year time limit. They are afraid that these bandits will just wait 1 year, and then use all of this information, that will bring them great profit.

Would you promise, Mr. Smith, to give these people a lifetime monitoring service, and instant email and postal alerts for each and every consumer who has been victimized as a result of ChoicePoint's negligence?

Mr. SMITH. Well, we will continue to look at other remedies. To date, that was, as people—we were trying to understand what was a reasonable amount of time to be done. We chose that particular period. To the extent that we should review that, or consider it, we will do so.

Mr. MARKEY. Would you give them 10 years? One year just isn't enough time. Will you give them 5 years?

Mr. SMITH. I would be pleased to work with you and others of the committee, to find a way——

Mr. MARKEY. No, no, no, no, no, no, no. I want to know right now. One year is not long enough. Will you give them more than 1 year? Will you give them 2 years?

Mr. SMITH. We will consider extending the period of time.

Mr. MARKEY. I know your lawyers said to make no concessions. One year is too short, Mr. Smith. What do you think? What do you think is a reasonable time? Do you think 1 year is a reasonable time, Mr. Smith?

Mr. SMITH. What I would say is I share your concern, and I will look at—to try to determine what is a reasonable amount——

Mr. MARKEY. What do you think——

Mr. SMITH. [continuing] to extend that.

Mr. MARKEY. Would you think 1 year is reasonable? You already made that decision. Now that you think about it, do you think 1 year is too short or not, Mr. Smith?

Mr. SMITH. Well, I can tell you that I personally was a victim of identity theft.

Mr. MARKEY. All right. So what do you think?

Mr. SMITH. So I conclude that——

Mr. MARKEY. Do you think—do you want these thieves to have your name now for than—do you think after a year, that they are not going to use it? Or do you think that you don't want them, maybe, for 5 years, to have some kind of notice that you are getting back that it is being compromised, Mr. Smith?

Mr. SMITH. Well, I mean, identity theft is obviously a very, you know, serious crime.

Mr. MARKEY. Right. So give us more than 1 year. Give these people, give my constituents more than 1 year. Can you give them 2 years, Mr. Smith?

Mr. SMITH. As I said, I—we will take a very hard look——

Mr. MARKEY. No, no. I want you, you run the shop. Will you give them more than 1 year, Mr. Smith? I don't want you to take it under advisement. You have been thinking about this your whole career. This is your business. You don't need any more time to think about it. Is 1 year enough time, or should they get more than 1 year——

Mr. SMITH. It was——

Mr. MARKEY. [continuing] in terms of the protection that they get?

Mr. SMITH. It was our opinion at the time that 1 year was a reasonable and responsible thing to do.

Mr. MARKEY. You think 1 year is reasonable and responsible.

Mr. SMITH. I think, given what I know today, it is, but I would be glad to, you know——

Mr. MARKEY. It sounds like you are not going to change, then, Mr. Smith. Let me—and I don't think that is a good answer for this committee, and I don't think you should be coming in here letting us think that 1 year is enough time, when these people can just sit, lay in wait, while the 1 year statute of limitations runs, and then they are off with 145,000 names, okay? That is just absolutely preposterous.

Now, what types of personal information has been compromised? You just said in the letter to my constituent, "personally identifiable information, such as your name, address, or Social Security number may have been viewed by unauthorized individuals." Why can't you tell my constituents whether or not it is their bank numbers, their credit card numbers, their passwords, their children's names and ages, passport numbers, home addresses, Social Security numbers, and similar private information? Will you give my constituents and all people affected exactly what personal information was compromised, and not this vague letter telling them that it could include all of this, but we are not going to give you the exact information.

Will you give them the specific information that has been compromised, and give all 145,000 people that specific information, Mr. Smith?

Mr. SMITH. Well, if they request this—again, we had to recreate the searches that were done, but if they would like the specific information that was on that report, that could—potentially could have been used, then we will provide that information to them, yes.

Mr. MARKEY. Well, why won't you just provide it to all of them as a matter of course? That is, the information that has been compromised? Why won't you just give each person that information, so they will know?

Mr. SMITH. Well, again, you have got to be—for their own benefit, you have got to be careful in how you disseminate that particular information. By simply sending that information out, you put it back in the public domain, where——

Mr. MARKEY. Will you give a notification to each and every person whose information has been compromised? The notice that you will provide to them if they ask you for it, each and every piece of information which will have been compromised, will you give them that notice that you will do this search for them and provide it to them?

Mr. SMITH. To the extent that we can do that, because we had to go back and recreate the search, and to the extent that that doesn't compromise any law enforcement investigation that is going on, then we would be willing to do that.

Mr. MARKEY. You will provide that information, and you—will you notify them that they—that you will provide it for them?

Mr. SMITH. Given our ability to recreate the search, and our ability to make sure we don't compromise law enforcement, we will do that.

Mr. MARKEY. Do you believe that there should be a ban on the sale of Social Security numbers?

Mr. SMITH. Again, I—my position is basically the same as the Chairperson of the FTC, in the sense that Social Security numbers, for the most part, should be restricted. There are certain uses——

Mr. MARKEY. No, no, I am talking about——

Mr. SMITH. [continuing] of that information——

Mr. MARKEY. [continuing] the sale of Social Security numbers. That is it. Just on the sale of Social Security numbers. Would you support the ban on the sale of Social Security numbers?

Mr. SMITH. Again, I would have to better understand the definition of sale, and how it is being done. But I don't support——

Mr. MARKEY. Mr. Smith, you—this is your field. You are an expert in this field. Let us—I am talking about, plain and simple, the sale of Social Security numbers.

Mr. SMITH. Well, there are certain circumstances where the sale of those numbers are, in fact, in the consumer's best interest, and so to the extent that that is correct, just the direct sale of a Social Security number, without a consumer benefit being derived associated with it, I am against that.

Mr. MARKEY. Give me one instance where you think the sale of a Social Security number would be appropriate. The sale of it.

Mr. SMITH. Well, I mean, there are cases where you are reviewing fraudulent circumstances associated with somebody's account, and you want to make sure that you have got the appropriate person, and you are matching them with the appropriate fraudulent circumstances——

Mr. MARKEY. And who would you sell this number to? Who—to whom could this number be sold, in your opinion?

Mr. SMITH. Well, it could be potentially used by law enforcement people. It could be used——

Mr. MARKEY. No, no, no. I am talking about the sale of the number. To whom do you think my Social Security number, my Social Security number could ever be sold, Mr. Smith? Who do you think it would be appropriate for you to sell it to? Sell it to.

Mr. SMITH. Well, again——

Mr. MARKEY. Not law enforcement, not information given to a police officer pursuant to a legally obtained warrant. Who else besides a law enforcement official, in your opinion, Mr. Smith, could you, or should you be allowed to sell my Social Security number to?

Mr. SMITH. Again, it is used when—and you have been in a position to be defrauded by somebody. It could be an authentication transaction, where I am trying to determine whether or not you have, in fact, been a victim of identity——

Mr. MARKEY. I am talking about selling my number as a product. Who do you think you should be allowed to sell it to, Mr. Smith?

Mr. SMITH. Well, again, if somebody is trying to determine whether or not there is a fraudulent transaction against your thing, they, in essence, get access to that Social Security number as part of a broader-based service. So I don't know whether you determine that a sale or not, but to the extent that we derive income

from the use of that information, I don't know if that is what you determine a sale or not.

Mr. MARKEY. Mr. Sanford, would you oppose the sale, would you oppose—would you support or oppose a ban on the sale of Social Security numbers of ordinary Americans?

Mr. SANFORD. I would not support a blanket ban on the sale of Social Security numbers, as you are describing. I think financial institutions need unique identifying Social Security number information when they are investigating fraud, making sure that they are doing business with the right individuals. I think law enforcement needs access to Social Security numbers. Businesses that are collecting legitimate debts, you need unique Social Security number identifying information to do their jobs.

Mr. MARKEY. Do you feel that I, or any American, has a right to know that you have transferred my Social Security number to a financial institution, which is now doing an investigation of me? Do you have a responsibility to give me a notification that you have transferred my number for that purpose?

Mr. SANFORD. Sir——

Mr. MARKEY. Do you think you should have a responsibility to notify an individual that my information, or any American's information, has been transferred to another party without my explicit permission?

Mr. SANFORD. No, I do not, sir. I think that the laws of the United States clearly lay out the permissible purposes for which sensitive information like Social Security numbers can be used. This deliberative body has decided what those legitimate and permissive uses are, and we responsibly use the information that is charged to us, to provide for permissible uses to, in fact, help consumers.

Mr. MARKEY. Well, the question is not whether or not the laws that have already been passed are adequate. The question is—are sufficient. The question is going forward, and learning the lessons which we have learned, should we have tougher protections on the use of Social Security numbers by companies that collect them?

My opinion is, Mr. Chairman, that what we are hearing today is basically an industry that is still in denial. It still doesn't recognize how highly all Americans value their privacy, and will hope to be able to ride out this scandal, without having Congress have made the changes that are necessary, and all I know is that Mr. Smith and his company are the largest single contributors to a lobbying effort to block truly effective privacy laws being passed in Congress. And that is all I have to know, okay? Because we are not going to have a discussion with him as he sits here, because his company is, in fact, effectively the chief lobbyist to block any effective privacy laws from being passed, and we are not going to get the answers we need for the public at this hearing.

Mr. STEARNS. The gentleman's time has expired. I would say to all members we might go a second round, if people feel strongly about it. We don't have a lot of members here. We have the time allotted for it. The gentleman—Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. A question for Mr. Smith. I wasn't real clear when you were answering Ms. Baldwin's question, Mr. Smith. In your testimony, it says "we have

decided to exit the consumer-sensitive data market not covered by the Fair Credit Reporting Act." And you explained some of that, about someone affirmatively asking for something that benefits the consumer, and so on.

The incident in California, had you had that in place, that person would not have qualified for that information?

Mr. SMITH. The information on that particular report would not have had the driver's license or, in fact, the Social Security numbers on it under that situation. That is correct.

Mr. GONZALEZ. So what you have in place, you would avoid certain information having been transmitted to this fraudulent business that was requesting your services.

Mr. SMITH. That is correct.

Mr. GONZALEZ. What is—where do you get all this information? I am just curious. I know public record is public record, and I think Mr. Sanford has alluded to it, and we all know that. Once it is in the basic public domain, you collect it, disseminate it, and so on. But what are your sources for the Social Security numbers, Texas driver's license numbers, that type, that is not generally made public?

Where do you get all that information? And I am not—Mr. Sanford, Mr. Smith.

Mr. SMITH. Well, I mean, the information comes from a myriad of sources. It comes from basic Federal, State, and local data repositories. It comes from—in terms of our Fair Credit Reporting Act business, it comes from the insurance industry itself. It comes, in some cases, from the consumers themselves, and information that they have provided.

So there are a tremendous myriad of sources of the raw data, that we either directly acquire or we get through conduits for things such as the Fair Credit Reporting Act, and get credit reports through the credit reporting agencies.

Mr. GONZALEZ. Okay. And you have indicated in your testimony that maybe there were some red flags, you should have acted more quickly in responding to what happened in California. Is that correct?

Mr. SMITH. Now that we understand that situation, and how it evolved, we should have recognized sooner the magnitude of that particular crime, and escalated the processed to a greater extent. That is correct.

Mr. GONZALEZ. I am not familiar with specifics. Was this just one individual company fraudulently operating that got 145,000 records or information on individuals?

Mr. SMITH. In this particular case, it was—I mean, this is an active law enforcement investigation, so I really can't talk in great detail.

Mr. GONZALEZ. Oh, you won't compromise anything, believe me.

Mr. SMITH. But the crime itself, but in essence, an individual was able to get a legitimate, but unfortunately fraudulent California business license, that was——

Mr. GONZALEZ. One business license——

Mr. SMITH. It was——

Mr. GONZALEZ. [continuing] with regard to 145,000——

Mr. SMITH. [continuing] with a business license, and then, they were able to get subsequent account structures under either that business license, or other fraudulent licenses associate with that particular situation. It depends on the type of small business in which you are, it would ring a flag in terms of whether or not 145,000 or whatever the specific number was in that case, would be abnormal or not. Historically, there would have been sometimes, collection agencies, for instance, would be using the information to help find people who were due bad debts.

Mr. GONZALEZ. So it was not unusual to have that kind of number, in the way of requests, from any particular entity.

Mr. SMITH. It depends on what the customer, the type of business in which that customer was, and in particular, the type of permissible purpose or access purpose in which they were granted. You know, again, I would remind you that it was through our audit processes, in this particular circumstance, that we found that it appeared to be usage that was outside of what would have been the normal patterns of this particular circumstance, that ultimately led to the investigation in California itself.

Mr. GONZALEZ. Okay. Let me ask you something quickly. And I am not real sure—I know it means a lot of work for you and such. If someone is making an inquiry on Congressman Gene Green, because someone—obviously, someone stole his briefcase. It could be identity theft. Is there a problem notifying the individual that an inquiry is being made by ABC Company, Wells Fargo, or whatever, just basically Congressman Gene Green, you are notified that our company has been requested to provide certain information to Company ABC. Because then Gene would know he has never gone into ABC Company. He has never made an application for any type of—there is no type of transaction relationship, transactional relationship.

Mr. SMITH. Again, it would depend upon why that information was being accessed. Many times, it is being accessed to determine whether or not a fraudulent transaction or some other situation, where not necessarily you would want to let the consumer alerted to the fact that that information was being accessed. So there are some cases where there certainly would be nothing wrong with alerting to somebody that, in fact, their information had been accessed. But in other situations, that could, in essence, defeat the very purpose of why the information was being used.

Mr. GONZALEZ. And then, real quick, I think I am out of time. I only need a minute, Mr. Chairman. And that is, if you are a victim of identity theft, let us say Congressman Green had been a victim of it, and he is trying to clear up all his records.

Is it reflected in the information that you compile that someone is a victim? In other words, so there is future inquiries. Congressman Markey made a good point. You know, you have got 1 year running on this thing. I guarantee you that information has been sold, resold, it is all over the place. A year does nothing, and it is ongoing.

Is there anything that alerts you guys that gather all this information that this was a victim of identity theft, and things that may be, again, relevant to that file, or account, may be part of that fraudulent act?

Mr. SMITH. There is no centralized system that allows for that to take place. You can put a fraud alert on your credit report that would indicate, in fact, that you have been a victim of identity theft, which would change the nature of which that report was being viewed.

Mr. GONZALEZ. And that is not mandatory, that is just——

Mr. SMITH. That is an option that the consumer, and some consumers choose to take that option, and some consumers do not.

Mr. GONZALEZ. All right. Last question quickly. And what would it cost to get a report? I know that from the credit reporting agencies, that I am entitled to get a free report or whatever it is, is it also free from ChoicePoint?

Mr. SMITH. It is. It is governed, again, those particular reports, on the Fair Credit Reporting Act, and you are entitled to a free report on an annual basis.

Mr. GONZALEZ. Thank you. Thank you, Mr. Chairman.

Mr. STEARNS. The gentleman——

Mr. STRICKLAND. Mr. Chairman—oh.

Mr. STEARNS. Yes.

Mr. STRICKLAND. I was just going to—expanding Mr. Gonzalez's last question——

Mr. STEARNS. Do you seek additional—unanimous consent?

Mr. STRICKLAND. The unanimous consent. Is that report that is at no cost similar to what we would get from a credit reporting agency, or would it be the expanded report, or the comprehensive report, that I know that was quoted in the MSNBC article?

Mr. SMITH. The public record report is not governed under the Fair Credit Reporting Act, and so that would be a separate report, in terms to be able to gain access to that report.

Mr. STRICKLAND. Although you package that into a comprehensive report for someone who subscribes to the service?

Mr. SMITH. Well, no, that is just a technical name of a public record report. That is not packaged together with those other types of reports that are covered under the Fair Credit Reporting Act. It is just—that is just a term used for a specific type of public record report.

Mr. STRICKLAND. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman.

Mr. STRICKLAND. Just trying to get our definitions right. Thank you. The full chairman of the committee.

Mr. STEARNS. The full chairman is recognized.

Chairman BARTON. Well, thank you. And of course, Congressman Gonzalez just left, but we were in the enviable position just then, that Ranking Member Schakowsky and subcommittee Chairman Stearns were so lucky to be surrounded by three Texans on the right and the left. Sometimes, it is just fun to be alive in this committee, isn't it? There you go.

I want to first thank you two gentlemen for testifying voluntarily. You know, we didn't have to subpoena you, and we were able to work with your representatives to make sure that you all could come, and felt comfortable coming. So I do want to publicly on the record thank you for that.

I am going to ask one of the same questions that Congressman Markey asked in his questions. I am really wrestling with this

issue of selling people's Social Security numbers without their permission, and I asked this to the Chairwoman of the Federal Trade Commission, and she has indicated that she—if I heard her correctly, she didn't think it should be traded or sold without the permission of the individual, unless there was a law enforcement reason to do that.

So I wanted to give you two folks, since you are two of the biggest data collectors in the country, an opportunity to tell why, if you do think it should be legal to continue to sell the Social Security number, without the permission of the individual, why that is so.

Mr. SANFORD. Would you like me to go first?

Chairman BARTON. Either one.

Mr. SANFORD. All right. Chairman Barton, a Social Security number is a particular unique identifying number, and there are some Federal laws that govern the use of that, and which provide for legally permissible uses. The intent of that law was to facilitate commerce, to help law enforcement. And in addition to law enforcement situations, having the ability to actually associate broad records and information with a particular individual, that Social Security number is that unique identifying piece of information that allows financial institutions, for example, to determine whether or not they are having a fraudulent transaction in their business.

It clearly is critical for law enforcement. It is critical, also, in the collection of debts, collection of debts for companies. It is very, very important in terms of keeping costs down for the rest of the consumer. We restrict the use of Social Security numbers in our data bases for these specific permissive uses. At LexisNexis, we truncate the Social Security number, the last 4 digits, so that unless you have a specific permissible use, under Federal law, you will not see that Social Security number displayed in the answer for a query that you do on the system.

We are also extending that kind of masking to sensitive other information, like driver's license numbers, and our restrictions are more restrictive than what is currently required by law. I think that strikes the right balance, in terms of making sure that we provide for lawful, legitimate uses of this information, but at the same time, protecting the privacy of the consumers.

Chairman BARTON. Okay. Mr. Smith.

Mr. SMITH. Well, first, you know, I would say that I do support stronger legislation regarding the uses of Social Security numbers, in particular, in the display of those Social Security numbers, so that while they may need to be used to validate and verify an individual, or help support a transaction, the actual printing out of those numbers, or at least certainly in their totality, I don't believe is a necessary thing to do, and could be restricted in very dramatic ways.

I think what you hear coming from at least me, and I think, you know, my colleague shares this, is that there are more than 23,000 William Smiths in the United States, and as we try, and society tries to determine how you can legitimately determine one individual from another, or particularly, to ensure that their data is correctly put with that individual and another, people who are try-

ing to find appropriate mechanisms to create the uniqueness of that individual. One of the mechanisms that has been used to do that has been the Social Security number. Others, driver's licenses, so that—and what we are trying to suggest is that there needs to be a recognition that the ability to use some type of personal identifier, whatever correct one it is. If you could get to a better, more specific one, and not use Social Security numbers, that would be terrific, so that you can make sure that you are dealing with that unique individual.

As William Smith moves around statistically, will move around the United States, 15 percent of them will move, you want to make sure that you put the data with the correct one. So I agree, the publishing and making available for anybody to see a Social Security number is not an appropriate thing to do. We just need to make sure that we can maintain the uniqueness of individuals, and allow for those applications, such as fraud or law enforcement, where it provides a very important tool.

Chairman BARTON. Well, I don't want to belabor the point, and we didn't do this for this hearing, but I thought about it, to prove a point. I could have asked the staff to take your two names, and without too much trouble, gotten your Social Security number, and with that, gotten lots of information out there that is collated on you two gentlemen. A lot of it, I didn't need to know, you know, just almost for prurient interest, to get a profile on you two gentlemen. Just to prove—now, I didn't do that, because that would have been kind of hitting below the belt, but it is—it would have been easily done. And that is wrong.

You know, we had banks long before we had the Social Security system, and bankers made loans, and bankers checked up, and we had fraud long before the Internet, but the Internet has made fraud a lot easier to commit, and you two folks are in the business of collecting information, which is totally legitimate, but sometimes, the information you collect, when people apply to get that information, they apparently use this loophole of trying to prevent fraud. They want to—and you sell them the information totally legally, not illegal, but they don't use it for that purpose, and you folks don't make any real attempt to try to guarantee that it is used for the purpose for which you allegedly, they purportedly ask that you give it to them, and I think that is just wrong.

I mean, we have got to find a way to allow you folks to do what you do, and protect the privacy of the average citizen, and I am not sure what we are going to do, but I think there is a very good chance we are going to put together a bill that will make it illegal to sell the Social Security number without the permission of the individual, unless there is a legitimate law enforcement purpose, or there may be one or two other exceptions. I don't know what they would be. I have just—I have not heard anything that explains to me why we should allow that to go on.

Mr. Chairman, I have exceeded my time. Thank you.

Mr. STEARNS. I thank the full chairman. Let me just, we are going to allow a second round here, if the chairman wishes. But let me just follow up a little bit with what the chairman mentioned. And with Mr. Markey. He was trying to ask you specifically to give us a case example when you could sell the Social Security number,

and I would like each of you just to take John Doe, for example. Under what circumstances would you sell the Social Security number for John Doe? Just give me specifically what that would be, each of you.

Mr. SANFORD. Well, would you like a law enforcement example?

Mr. STEARNS. Well, let us—okay.

Mr. SANFORD. Or a financial institution example?

Mr. STEARNS. For selling, would you—do you actually sell to the law enforcement, do the——

Mr. SANFORD. What we——

Mr. STEARNS. Does the FBI and the Justice Department pay you for the Social Security numbers for John Doe?

Mr. SANFORD. We enter into subscription agreements at LexisNexis with——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] law enforcement agencies, financial institutions. They are subscribers——

Mr. STEARNS. Financial institution means banks.

Mr. SANFORD. Yes, sir.

Mr. STEARNS. All the banks in America. If they——

Mr. SANFORD. That would be our hope.

Mr. STEARNS. Yeah, if they——

Mr. SANFORD. Not yet.

Mr. STEARNS. [continuing] subscribe. Okay. Financial institutions, law enforcement, who else?

Mr. SANFORD. You would have credit departments of legitimate businesses who are trying to collect legitimate——

Mr. STEARNS. Right.

Mr. SANFORD. [continuing] debts of——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] that organization. And then, on a case by case basis, you could have a particular, you could have a particular organization——

Mr. STEARNS. Could this——

Mr. SANFORD. [continuing] a government body who is investigating——

Mr. STEARNS. Yeah.

Mr. SANFORD. [continuing] criminal or fraudulent activity.

Mr. STEARNS. Well, let us say Chairman Barton wanted to get the Social Security number for John Doe. Could he pay you?

Mr. SANFORD. He would have to have a—one of the permissive uses, and not just because he wanted to look it up. He would not gain access.

Mr. STEARNS. But if he had the permissive—permitted uses, he could buy it from you.

Mr. SANFORD. He would, as part of a subscription agreement——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] do a query on the service, and he would get an answer.

Mr. STEARNS. Okay.

Mr. SANFORD. And if he was——

Mr. STEARNS. So let us say he goes out and opens up a business. He gets a business license, and he calls himself whatever is necessary to get this permitted use, then you would give it to him.

Mr. SANFORD. Well, I would like to tell you that our verification procedures are not going to allow someone like that to gain access, first of all, even to a—that kind of information. We have a very, very rigorous verification authentication process. And then, just because we credentialed you, and we are willing even to do business with you, then we go through a special access credentialing to make sure that you have legitimate purposes.

Just because you are a bank doesn't mean we are automatically going to——

Mr. STEARNS. But in the case of ChoicePoint, they did all this, and it still didn't work, and this person got the Social Security numbers, right? That is what happened.

Mr. SANFORD. Well, we are never going to—I can't guarantee you that——

Mr. STEARNS. So——

Mr. SANFORD. Sir, I can't guarantee you that——

Mr. STEARNS. So you are credentialing Chairman Barton to get John Doe's Social Security number is the key. If that credentialing is not done rigorously, robust, then for all intents and purposes, that Social Security number is being sold and being used—the key is that credentialing, don't you think?

Mr. SANFORD. I think it is one of the keys. I think there is actually a lot more to it than that.

Mr. STEARNS. Okay.

Mr. SANFORD. I think credentialing is the first step. I think strong security protocols is the second step. Making sure that companies that would appear to be legitimate businesses still have a need, have a permissive use to use that, and then, ongoing monitoring and security to make sure that the usage by those customers is not abnormal. Detection software that people like us use to monitor to see whether or not we have abnormal usage.

Mr. STEARNS. Now, I am not suggesting this, but is there a possibility that we need an outside third party to credential your credential? In other words, the credential is between you and Chairman Barton in this case. Is it possible that we need some kind of corroboration, authentication of what, how you credential these people, some standards, or the fair—I mean, I don't know. I mean, just your—I mean, I am just asking whether——

Mr. SANFORD. Yeah. I mean, we contract ourselves with third parties to conduct security audits——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] to advise us. We talk to law enforcement. We ask them what else should we be doing, not just in this current——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] situation, where we have——

Mr. STEARNS. Okay.

Mr. SANFORD. [continuing] an investigation——

Mr. STEARNS. All right.

Mr. SANFORD. [continuing] ongoing.

Mr. STEARNS. Mr. Smith, you have written a book called Risk Revolution, and you have talked about how information technology can be used to reduce risk and increase peace of mind, and you also talk about personal privacy and how we need to—need not trade

civil liberties for civil defense, if we act now, in this book called risk. But one of your quotes in the book is, it says: "Each of us have a right to privacy. However, none of us have a right to absolute anonymity." And could you explain that, what you mean by——

Mr. SMITH. Yes.

Mr. STEARNS. [continuing] that expression?

Mr. SMITH. I will be glad to. What I am saying is is that as people seek rights and privileges in society, for instance, you are trying to drive a hazardous waste truck through the Holland Tunnel in New York, where you could potentially put millions of people at risk, then your ability to be anonymous, or not having to disclose who you are, when you are trying to get that particular right or privilege, is something that I think in today's risky world, would be extraordinarily problematic, and would create more problems than it would solve.

Mr. STEARNS. So any American who wants to be anonymous cannot be so, in your—he will not have this absolute——

Mr. SMITH. No.

Mr. STEARNS. [continuing] anonymity, because he cannot have it, in your expression?

Mr. SMITH. No. Not at all. If you are sitting at a sidewalk café, and you are not seeking any right or privilege from society, or you are not at any risk to anyone else, then I absolutely don't believe that people should have the right to know who you are. This is more as you interact throughout society, because there are risks that are being created every day, and to give you an example, 3 percent of all volunteer workers today have undisclosed serious criminal violations, and just recently, we had a situation where, in Texas, in fact, where somebody was applying to be a volunteer at a youth, female youth organization, who had just been released for his eighth conviction of child molestation 2 weeks prior to him trying to volunteer. That is a circumstance and situation where we can't allow someone to be anonymous and put our children at risk. That is the kind of situation in which I was referring to in the book.

Mr. STEARNS. All right. Thank you. And the gentlelady.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. Our subcommittee asked both of you to submit sample reports, that can be redacted reports, for the record. And I wanted to be sure that you are going to provide us with that information.

Mr. SMITH. I didn't know we were asked to. Go ahead.

Mr. SANFORD. I apologize. I understand we have not yet submitted that. Chairman Stearns and I talked about my attendance on Thursday, last week, so I am sure we will get you that in a matter of days.

Ms. SCHAKOWSKY. And Mr. Smith.

Mr. SMITH. We would be pleased to do that.

Ms. SCHAKOWSKY. You act as if you don't know that you were asked for it.

Mr. SMITH. I checked—I was not aware personally that we were asked for that.

Ms. SCHAKOWSKY. Okay. Well——

Mr. SMITH. But we would be pleased to do so.

Ms. SCHAKOWSKY. Okay. Thank you. I have a number of questions I wanted to ask. Mr. Smith, how much does it cost you to provide that information for—to provide that monitoring for a year? How much is your company going to expend per year to try and protect those whose privacy was breached?

Mr. SMITH. That is a two—it approaches $2 million.

Ms. SCHAKOWSKY. Okay. And Mr. Smith, how much did your company spend last year—well, let me just read you the quote from the Wall Street Journal. "These data sellers," and I am assuming that would include LexisNexis, I am not sure, "have developed a deft combination of lobbying and industry-affiliated think tanks to head off increased oversight. ChoicePoint, and six of the country's other largest sellers of private consumer data, spent at least $2.4 million last year to lobby Members of Congress in a variety of Federal agencies, according to disclosure forms filed with the U.S. House and Senate. ChoicePoint was the biggest spender, with $970,000 either paid to outside lobbyists, or spent directly by the company." And let me just make an editorial comment here. You know, at the same time as you are saying that now, after the fact, you want to help these consumers, your company, at least, and I don't know about Mr. Sanford's, are engaged in lobbying efforts to defeat increased oversight, to the tune, it appears, of about $1 million last year.

Mr. SMITH. Well, it is my understanding that the majority of the dollars you just spent there were not spent in lobbying for no regulation in our industry. A lot of that was done for business development here in Washington. We serve a lot of clients in this particular area. I mean, I would be glad to get you a more accurate data as to what was done lobbying-wise. I would——

Ms. SCHAKOWSKY. Well, I—let me ask you this. If both of you could provide us with information on positions that you have taken on legislation that has dealt—or regulations that have dealt with privacy, I would appreciate seeing that information.

Let me ask one final question that deals with victims of domestic violence. I wondered if either of your companies make any special efforts—I actually don't know if you are required by law, if you voluntarily do anything to protect the information of domestic violence victims?

Mr. SMITH. I will have to get back with you to answer this. I don't believe so, but I don't know the answer to your question.

Ms. SCHAKOWSKY. You realize what I am getting at, that the fact that this information, even as basic information as address, could put the lives of people who have been victims of domestic violence at risk.

Mr. SMITH. Well, we take domestic violence very seriously. We sponsored the National Rape Evidence Project, in which we raised, as a company, over $200,000 to help get rape kits tested——

Ms. SCHAKOWSKY. Well, sorry, but——

Mr. SMITH. [continuing] the police, yeah, so this is an issue that we believe very strongly in, and so we support you in any way, in order to make sure that in no circumstance, somebody could be subject to violence as a result of this information.

Ms. SCHAKOWSKY. So you—I would hope that, then, you would check what policies you have to prevent, and Mr. Sanford.

Mr. SANFORD. Yes, we have a policy that under limited situations, individual consumers can opt out of our data bases, and that is actually one of the examples where people do opt out, because making their identity known to others, then, would put them at future risk.

Ms. SCHAKOWSKY. How would one opt out?

Mr. SANFORD. I have on our LexisNexis website, we have a privacy page that lays out the procedures, who they call, and they usually submit documentation. It lays out, you know, what is the reason.

Ms. SCHAKOWSKY. How would someone know to do that? How would someone that is a victim of domestic violence know how to avail themselves of that option?

Mr. SANFORD. I think unless a consumer agency or a counselor made them aware of it, they probably wouldn't know.

Ms. SCHAKOWSKY. Thank you.

Mr. STEARNS. I thank both of you for your time and forbearance here. We are completed with the second panel, and we invite the third panel to come forward.

Mr. Joseph Ansanelli, Chairman and Chief Executive Officer of Vontu, Incorporated, and Mr. Marc Rotenberg, Executive Director, Electronic Privacy Information Center. We welcome both of you, and thank you for your patience for waiting through the second panel.

And Mr. Ansanelli, we will start with you, with your opening statement.

STATEMENTS OF JOSEPH ANSANELLI, CHIEF EXECUTIVE OFFICER, VONTU, INC.; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ANSANELLI. Chairman Stearns, Ranking Member Schakowsky, and members of the committee, good afternoon, and thank you for inviting me to testify, and thank you for your ongoing efforts and focus on this issue of the protection of consumer data. I am Joseph Ansanelli, CEO of Vontu. We provide information security solutions to help Fortune 500 companies, such as Best Buy, Prudential, Charles Schwab, and others prevent the loss of consumer data over the Internet.

Given my work with these companies, I hope to provide a unique viewpoint for policy considerations, and add to the discussion of a need for a national consumer data security standard. In order to reduce identity theft, it seems that there are at least three important areas for policy.

The first is the criminals who actually steal the identities. Second is the consumers who need education on the importance of protecting their identities, as well as help if they become victims. And the third area is the organizations that actually store consumer data. It is third area, companies, businesses, government agencies that store consumer data, in which I have particular expertise, and is the focus of my testimony.

An important point to understand is that these organizations are not the criminals perpetrating identity theft. In fact, all the companies with which I work invest significant resources, and are fully committed, to protecting consumer information. However, today,

the question that many people are asking is are these organizations doing enough to ensure the security of consumer data?

To answer that question, I suggest we must first ask the question, is it clear to these organizations what is required and expected of them to ensure the security of consumer data? Unfortunately, despite existing legislation, there is some confusion around what is required, and confusion is the enemy of consumer protection. To date, Congress has taken important steps to address consumer data protection, through industry and organization-specific regulations. For example, Congress has passed Section 501(b) of Gramm-Leach-Bliley for financial services, Part 164, subpart C of HIPAA for healthcare providers, the Driver's Privacy Protection Act, the Fair Credit Reporting and FACT Act, and many others. Additionally, many States are creating de facto national standards and requirements, such as California S.B.1386, which requires notification in the case of a breach. These different legislative acts have—all have aspects of consumer data protection, yet each has tackled the problem differently, based on either industry or State-specific requirements. And that is where the confusion begins.

I think one important question for this committee to consider is what is the difference in how a bank versus how a retailer, versus how a utility provider should treat the security of a Social Security number or any other consumer information, and should the focus of policy be on the industry, or instead, on the data itself? I think everyone would agree that the data is what needs to be protected across all industries. We support the suggestion of the Chairwoman of the FTC earlier today that one possible solution to raise the level of consumer data protection is to extend existing regulations, such as GLBA, and the Safeguard Rules, to any organization which stores data. This would enable and create a preemptive and unified national consumer data security standard. We suggest the standard would require organizations that store nonpublic consumer information to one, ensure the security of that information. This would create an affirmative obligation of companies that store it to protect it.

Second, we think that organizations should protect against reasonably anticipated threats to the security of such data. As new threats emerge, this would allow the requirements to evolve without requiring new legislation. Third, it is important that companies protect against unauthorized access to or use of such information that could result in substantial harm to a consumer. This would help prevent against fraudulent efforts to gain access to the data by outsiders or insiders, as is the case in many recent breaches. Fourth, we think that companies have an obligation, and should have an obligation, to ensure compliance with their security policies by both their employees and workforce, as well as third parties that they give access to that information.

This would help address the issue of the insider threat, which was the situation in the recent Teledata case, as well as concerns regarding offshoring and outsourcing. These first four are very similar to what is currently required under GLBA and HIPAA.

The last requirement we suggest and we support is the idea of notification. Companies should disclose any loss of information, when it is reasonably believed that such loss could result in sub-

stantial harm to the consumer. This would clearly help consumers proactively protect themselves by monitoring their credit reports, setting up fraud alerts, and other efforts to watch for potential issues.

In addition, while these requirements serve as the proverbial stick, I suggest the committee also consider any new legislation also potentially provide a carrot as an incentive to go beyond any base requirements. It is important to remember that security is a journey, and like any other crime, it is unlikely we will completely eliminate the theft of identities. Therefore, a carrot might provide some level of protection against the risk of excessive punitive damages for those organizations with qualifying security programs. This is not protection against economic or reasonable pain and suffering damages, but against excessive punitive actions when companies are already meeting or exceeding these requirements.

In summary, to reduce identity theft, policy should focus on the three areas of criminals, the consumers, and the organizations that store consumer data. I suggest this committee consider the idea of a preemptive national consumer data security standard that also protects organizations from potential excessive punitive damages, when they are making the best efforts to protect the data.

Thank you, and I look forward to any questions.

[The prepared statement of Joseph Ansanelli follows:]

PREPARED STATEMENT OF JOSEPH ANSANELLI, CHAIRMAN AND CEO, VONTU, INC.

Chairman Stearns, Ranking Member Schakowsky and all the Committee members, thank you for your ongoing focus on the protection of consumer data.

I am Joseph Ansanelli, CEO of Vontu, an information security solutions company that helps Fortune 500 organizations such as Best Buy, Prudential, Charles Schwab and others, prevent the loss of consumer data over the Internet. Given my experience with helping some of the largest companies in America protect their consumer data, I hope to provide a unique viewpoint on the question of policy considerations as a result of recent cases of consumer data loss and if there is a need for a national consumer data security standard.

PROBLEM: IDENTITY THEFT AFFECTS MILLIONS EVERY YEAR

The FTC[1] estimated that in one year alone approximately 10 million people—or almost 5% of the US adult population—were victims of Identity Theft. These victims reported $5 billion in out-of-pocket expenses and countless hours of lost time repairing their credit histories. In the previous five years, almost 30 million people were victims of identity theft.

This is not only a problem for consumers, but for business as well. As part of the same FTC report, the losses to businesses totaled nearly $50 billion.

Additionally, there is a risk to companies that is not mitigated through insurance or other strategies—loss of consumer trust. Vontu commissioned a survey[2] of 1000 consumers in the United States to better understand the effect that security of customer data has on consumer trust and commerce. Some of the findings include:

- **Security drives purchasing decisions**—More than 75 percent of consumers said security and privacy were important in their decisions from whom they purchase.
- **Consumers will speak with their wallets**—Fifty percent said that they would move their business to another company if they did not have confidence in a company's ability to protect their personal data.
- **Insider theft increases concerns about a company's data security efforts**—More than 50 percent of the consumers surveyed said an insider breach would cause them to be more concerned about how a company secures their information

[1] Federal Trade Commission—Identity Theft Survey Report, September, 2003

[2] Vontu Consumer Trust Survey, See Appendix 1

Clearly, financial costs and loss of consumer trust as a result of identity theft are a significant problem today.

IDENTITY THEFT POLICY IMPLICATIONS

In order to reduce Identity Theft, there are at least three areas of focus for policy:

1. Criminals who steal identities. This is important not only for reducing Identity Theft, but other crimes and threats to national security. Professor Judith Collins of Michigan Statue University's ID Theft Crime Lab states that virtually all identity thieves are involved in other felonies or terrorist acts. The Identity Theft Penalty Enhancement Act, which became law in July 2004, was a positive step in the right direction to increase the penalties and provide additional tools for law enforcement and the courts to punish those found guilty of identity theft.
2. Consumers who need continued education on the importance of protecting their identities and as well as help if they are victims. The efforts of the FTC with the ID Theft hotline, privacy website and on-going educational efforts are important and more can be done to raise awareness of those efforts. Additionally, the FACT Act provided much needed tools for consumers including free annual credit reports, the ability to place fraud alerts in their credit report, and ability to more easily correct inaccuracies in their credit report resulting from identity theft.
3. Organizations that store consumer data.

RESPONSIBILITY OF ORGANIZATIONS

The third area, companies, government agencies and organizations that store consumer data, is the one in which I have the most experience and is the focus of my testimony. An important point to understand, before we can truly begin to address the problem, is that these organizations are not the criminals perpetrating Identity Theft. In fact, all of the companies that I have worked with invest significant resources and are thoroughly committed in their efforts to protect consumer data.

However, we all recognize that organizations with consumer data are a crucial "link in the chain" to prevent identity theft and the question that many people are asking is:

> "Are these organizations doing enough to ensure the security of consumer data?"

To answer that question, I suggest one must first ask:

> "Is it clear to organizations what is expected of them to best protect consumer information?"

Unfortunately, despite existing legislation, there is confusion around what is required of organizations and confusion is the enemy of consumer protection.

CONFUSION IS THE ENEMY OF CONSUMER PROTECTION

To date, Congress has taken important steps to address consumer information protection through industry and organization specific regulations. For example, Section 501 (b) of Gramm Leach Bliley for financial services, PART 164—Subpart C of HIPAA for healthcare providers, the Driver's Privacy Protection Act for state DMVs, the Fair Credit Reporting and FACT Act, and others. Additionally, many states are creating de facto national requirements such as California SB 1386 which requires notification in the case of a breach.

These different legislative acts have aspects of consumer data protection yet each has tackled the problem differently based on industry or state specific requirements. And that is where the beginning of the confusion lies.

One important question for this committee to consider is:

> "What is the difference in how a bank versus a retailer versus a utility provider should treat the security of a social security number, and should the focus of policy be on the industry of the data itself?"

NATIONAL CONSUMER DATA SECURITY STANDARD

I am sure everyone would agree, it is the data that matters and needs to be protected across all industries. One possible solution to raise the level of consumer data protection is to extend existing industry specific consumer data protection requirements to cover any organization which stores private consumer data and create a preemptive and unified, National Consumer Data Security Standard.

One alternative would be very similar to GLBA and HIPAA[3] in addition to a requirement for notification. The difference is that it would apply to any organization that stores consumer information regardless of industry or location.

This standard would require any organization that stores non-public consumer data to:

1. Ensure the security and confidentiality of consumer information. This would create an affirmative obligation of the companies to protect the data.
2. Protect against any reasonably anticipated threats to the security of such information. This would allow the requirements to evolve as new threats emerge without new legislation.
3. Protect against unauthorized access to or use of such information that could result in substantial harm to a consumer. This would help prevent against fraudulent efforts to gain access to the data by outsiders or insiders as is the cause in many recent breaches.
4. Ensure compliance with their security policies by an organization's workforce and third parties who are given access to the information. This would address the issue of the insider threat, which was the situation in the recent Teledata case, as well as concerns regarding off shoring and outsourcing;
5. Disclose any loss of the information when it is reasonably believed that such loss could result in substantial harm to a consumer. This would help consumers to proactively protect themselves by monitoring their credit reports, setting up fraud alerts and other efforts to watch for potential issues.

Rule making for this legislation would exist in relevant agencies and I believe that the FTC has already done much of the work under the GLBA Safeguards Rule 16 CFR Part 314 and could apply this rule beyond entities covered under GLBA.

In addition, while these requirements serve as the proverbial "stick", I suggest the Committee consider any new legislation also provide a "carrot" as an inventive to go beyond any base requirements. This "carrot" might provide some level of protection against excessive punitive damages for those organizations with qualifying security programs. This is important to help remove existing and valid concerns that organizations have about increased litigation risk as they proactively uncover new threats with respect to consumer data security. This is not protection against economic or reasonable pain and suffering damages, but against excessive punitive actions when companies are clearly meeting and exceeding these requirements.

SUMMARY

In summary, to reduce identity theft policy must focus on the criminals, consumers and organizations that store the data.

I suggest this Committee consider the idea of a preemptive, national consumer data security standard that also protects organizations from potential excessive punitive damages when they are making best efforts to protect consumer information. The standard would clearly state what is required of an organization and encourage them to use their best efforts to improve the protection of consumer information and help to reduce Identity Theft.

APPENDIX 1: RELEVANT GLBA SECTION

Gramm Leach Blilely

TITLE V—PRIVACY

SUBTITLE A—DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

[3] See attached Appendix 2 and 3

APPENDIX 2: RELEVANT HIPAA SECTION

HIPAA Security Requirements

PART 164—SECURITY AND PRIVACY

SUBPART C SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

Section 164.306—*General requirements*

Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance with this subpart by its workforce.

ATTACHMENT 1: 2003 CONSUMER INFORMATION TRUST SURVEY

ATTACHMENT 2: HARRIS INTERACTIVE DATABASE SECURITY HIGHLIGHTS

ATTACHMENT 3: PONEMON RESEARCH ON DATA SECURITY BREACHES

ATTACHMENT 4: VONTU 2004 DATA SECURITY TRENDS REPORT

2003 CUSTOMER INFORMATION TRUST SURVEY

Those organizations that sit on the highest perch when it comes to customer trust have the farthest to fall if they lose that trust according to the 2003 Customer Information Trust Survey commissioned by security technology innovator Vontu, Inc.

Consumers have the greatest amount of trust that companies within the health care industry have measures in place to protect personal information from identity thieves. Web retailers and retailers scored near the bottom in consumer trust in a ranking of 14 major industries. However, even the companies that scored well with consumers can face serious financial consequences if security breaches within their organization lead to a loss of consumer trust. Some of the major findings of the survey are:

- Security is important in the purchasing decision. More than 75 percent of the consumers said security and privacy was important in their decisions from whom they purchase.
- Not all security breaches are equal in the eye of the customer. More than 54 percent said security breaches by insiders or employees, now one of the fastest growing contributors to identity theft, would have the greatest impact on their trust in an organization.
- Consumers choose with their wallets. Fifty percent said that they would move their business to another company if they did not have confidence in a company's ability to protect their personal data.

VONTU INFORMATION TRUST RANKINGS*

Hospital or Clinic 82%
Pharmacy 79%
Bank 78%
Charity/Religious Org. 78%
Airlines 60%
Car Rental Company 53%
Utility 48%
Credit Card Company 47%
Cable Company 42%
Restaurants 42%
Hotels 41%
Web Retailers 41%
Retail Stores 38%
Grocery Store 25%

* The Vontu Information Trust Rankings rate 14 major industries based on the level of trust consumers surveyed said they had that these organizations would protect personal information from identity theft.

Two examples of the questions from the survey are:

How important is privacy and security to your purchasing decision?

- Very important 19%
- Important 57%
- Not important 9%
- Unsure/No Comment 14%

If an insider (such as an employee of the company) stole your data rather than an outsider (such as a computer hacker), would it change your answers to previous question about trust?

- Yes—More concerned about insider 54%
- Yes—Less concerned about insider 12%
- No—No difference 17%
- Unsure/No comment 18%

©2003 Vontu Inc.

Mr. STEARNS. I thank the gentleman. Mr. Rotenberg, welcome.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Mr. Chairman, Congresswoman Schakowsky, members of the committee. Thank you so much for the opportunity to appear today. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center. We are a nonpartisan research organization here in Washington, and we have been before the committee before, and we thank you, Mr. Chairman, for holding this very important hearing today.

With all the news reporting of the ChoicePoint matter over the last several weeks, I think it is very important to keep in mind what actually happened here. This was not a computer hack. This was not a theft. ChoicePoint sold this information on American consumers to a criminal ring engaged in identity theft.

ChoicePoint is in the business of selling personal information about American consumers, and while many other companies in the last few weeks have reported significant security breaches, I think it is critical for the committee not to lose sight of what is at issue here.

Our organization, EPIC, wrote to the Federal Trade Commission in December, before any of this became public, and we urged the FTC to open an investigation into ChoicePoint's practices. We were concerned about whether current Federal privacy law, and particularly, the Fair Credit Reporting Act, adequately protected the privacy of American consumers. We were also concerned because it became increasingly aware to us that ChoicePoint had developed a number of products and services that seemed to us very similar to the type of information products that would otherwise be covered by the Fair Credit Reporting Act, but ChoicePoint had, in fact, artfully found ways to avoid Federal oversight. And so it seemed obvious to us that the Federal Trade Commission would open an investigation, and try to determine what, in fact, was happening with the personal information of American consumers.

I have to say, Mr. Chairman, I was very disappointed this morning, when I heard the Chairwoman of the FTC say that, in fact, they did not open the investigation until the after the incident was publicly reported. I don't think it can be the case that the Federal Trade Commission waits until they read about a matter in the morning newspaper before they pursue what we believe was a very

well-founded complaint that we had pursued at the Federal Trade Commission.

Now, there are a number of others points that I make in my testimony about the lessons that I believe we can draw from the ChoicePoint matter. One of the critical concerns that I know you have, sir, over the years, as we have talked about privacy legislation, is the need to show that there is actual harm to consumers. And I think here, with ChoicePoint, it should be clear that the absence of effective privacy protection leads to significant harms. In fact, the harm here, the harm of identity theft, is the No. 1 crime that American consumers face, and the crime is increasing, as the FTC's own reports show. Over the last 5 years, the level of identity theft in this country is becoming the No. 1 problem that American consumers have.

I think the question as to whether privacy protection is necessary to prevent consumer harm has simply been answered by the ChoicePoint matter. I think it is also important to understand that with ChoicePoint, unlike a lot of other American businesses, consumers do not have a direct relationship. They can't exercise market control, as they might with a bank or an insurer, or somebody else who might have a bad privacy policy. People say about the Internet, for example, if you don't like a website's privacy policy, you can go somewhere else. But with ChoicePoint, consumers have no such control to go somewhere else, because they have no direct relationship with that company that simply collects and sells personal information about them.

We know already that there are problems with the adequacy of privacy protection, and we think particularly in this industry, information brokers such as ChoicePoint have made clear the need for more effective privacy regulation.

I think it is also important to understand from the ChoicePoint episode just how important State legislation is. Now, this has been another consideration before this committee, and we fully understand why it may be the case that companies would prefer to have a single, uniform standard, rather than 50 different State laws, and of course, we have had this discussion in the past. But please don't lose sight of what happened here.

Because the State of California took the initiative, and said we are going to try a new, innovative approach, it wasn't a comprehensive law, by the way, it was merely notification. They simply told people after the fact, after the breach had occurred, that they might be at heightened risk of identity theft, and because of that, American consumers, and consumers, you know, all across the country, outside of California, who were also notified, will be able to respond more effectively to this threat.

And I think we have to keep this in mind, even a national notification standard should not prevent States from coming up with more innovative solutions. States may find certain ways of notification, maybe by electronic means, that turn out to be more effective than what can be done here in Washington. So there is a strong case, following from the ChoicePoint matter, I believe, to avoid Federal preemption.

Now, I would like to say just a couple of words about the proposals that have been discussed this morning, and again, express

a bit of concern that apparently, there has been some significant discussion between the Chair of the Federal Trade Commission, and the witnesses that have appeared before you, about what might be done. But there has been no discussion with the consumer organizations about what might be effective privacy legislation to respond in this situation.

The Chairwoman proposes, for example, the extension of the Gramm-Leach-Bliley security standards rule. Now, that is not a bad proposal, and we certainly wouldn't oppose it, but we think it is an inadequate proposal, because it simply deals with a security matter, and as I have made clear at the outset, we were talking about the routine sale of personal information on American consumers by an information broker. So an effective solution certainly must do something more than simply extend the security standard rule.

In similar fashion, we think the California notification law provides a good basis to notify consumers after the fact when a breach has occurred, and without preemption, we think that would be a sensible thing for the committee to support, but what we really believe needs to be done at this point is legislation that brings this industry within some type of Federal control, accountability, oversight, that will safeguard American consumers.

We think the legislation that Mr. Markey has introduced is a very sensible starting point, and we have made some proposals, in fact, about how that can be strengthened. We think it is important that the Federal Trade Commission take a proactive stand on these issues. It is not sufficient to create a circumstance where there may be privacy violations, and the FTC can effectively sit on that fact, and not provide the type of assurance that would be necessary to safeguard American consumers.

So in conclusion, Mr. Chairman, I thank you again for holding this hearing. It is extremely important, for the 150,000 American consumers who are today at a heightened risk of identity theft, that the Congress act swiftly and effectively to make sure that we have no future incidents like the one that has occurred recently.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, PRESIDENT, EPIC

Mr. Chairman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that you have convened this hearing today on protecting consumer's data and the policy issues raised by Choicepoint.

In my statement today, I will summarize the significance of the Choicepoint matter, discuss EPIC's efforts to bring public attention to the problem before the incident was known, suggest several lessons that can be drawn from this matter, and then make several specific recommendations.[1]

The main point of my testimony today is to make clear the extraordinary urgency of addressing the unregulated sale of personal information in the United States and how the data broker industry is contributing to the growing risk of identity theft in the United States. Whatever your views may be on the best general approach to

[1] Many other organizations have also played a critical role in drawing attention to the growing problem of identity theft. These include Consumers Union, the Identity Theft Resource Center, Privacy International, the Privacy Rights Clearinghouse, the Privacy Times, the US Public Interest Research Group, and the World Privacy Forum.

privacy protection, Choicepoint has made clear the need to regulate the information broker industry.

THE SIGNIFICANCE OF THE CHOICEPOINT MATTER

With all the news reporting of the last several weeks, it has often been difficult to tell exactly how a criminal ring engaged in identity theft obtained the records of at least 145,000 Americans. According to some reports, there was a computer "break-in. "Others described it as "theft."[2] In fact, Choicepoint simply sold the information.[3] This is Choicepoint's business and it is the business of other companies that are based primarily on the collection and sale of detailed information on American consumers. In this most recent case, the consequences of the sale were severe.

According to California police, at least 750 people have already suffered financial harm.[4] Investigators believe data on least 400,000 individuals may have been compromised.[5] Significantly, this was not an isolated incident. Although Choicepoint CEO Derek Smith said that the recent sale was the first of its kind, subsequent reports revealed that Choicepoint also sold similar information on 7,000 people to identity thieves in 2002 with losses over $1 million.[6] And no doubt, there may have been many disclosures before the California notification law went into effect as well as more recent disclosures of which that we are not yet aware.

The consumer harm that results from the wrongful disclosure of personal information is very clear. According to the Federal Trade Commission, last year 10 million Americans were affected by identity theft. Identity theft is the number one crime in the country. For the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency last year.[7] And there is every indication that the level of this crime is increasing.

Choicepoint is not the only company that has improperly disclosed personal information on Americans. Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the federal government, including many members of Congress.[8] Lexis-Nexis made available records from its Seisint division on 32,000 Americans to a criminal ring that exploited passwords of legitimate account holders.[9] DSW, a shoe company, announced that 103 of its 175 stores had customers' credit and debit card information improperly accessed.[10]

But there are factors that set Choicepoint apart and make clear the need for legislation for the information broker industry. First, Choicepoint is the largest information broker in the United Stares. The company has amassed more than 19 billion records and has acquired a large number of smaller companies that obtain everything from criminal history records and insurance claims to DNA databases. The private sector and increasingly government rely on the data provided by Choicepoint to determine whether Americans get home loans, are hired for jobs, obtain insurance, pass background checks, and qualify for government contracts.

Choicepoint has become the true invisible hand of the information economy. Its ability to determine the opportunities for American workers, consumers, and voters is without parallel.

Second, the Choicepoint databases are notoriously inaccurate. A recent article in MSNBC, "Choicepoint files found riddled with errors," recounts the extraordinary

---

[2] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.

[3] Robert O'Harrow Jr., "ID Theft Scam Hits D.C. Area Residents," Washington Post, Feb. 21, 2005, at A01.

[4] Bob Sullivan, "Data theft affects 145,000 nationwide," MSNBC, Feb. 18, 2005, *available at* http://www.msnbc.msn.com/id/6979897/.

[5] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.

[6] David Colker and Joseph Menn, "ChoicePoint CEO Had Denied Any Previous Breach of Database," Los Angeles Times, March 3, 2005, at A01.

[7] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2004," (Feb. 1, 2005), *available at* http://www.ftc.gov/opa/2005/02/top102005.htm.

[8] Robert Lemos, "Bank of America loses a million customer records," CNet News.com, Feb. 25, 2005, *available at* http://earthlink.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029__3-5590989.html?tag=st.rc.targ__mb.

[9] Jonathan Krim and Robert O'Harrow, Jr., "LexisNexis Reports Theft of Personal Data," Washingtonpost.com, March 9, 2005, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A19982-2005Mar9?language=printer.

[10] Associated Press, "Credit Information Stolen From DSW Stores," March 9, 2005, *available at* http://abcnews.go.com/Business/wireStory?id=563932&CMP=OTC-RSSFeeds0312.

errors in just one Choicepoint report that was provided to a privacy expert.[11] Among the statements in the 20-page National Comprehensive Report was an inaccurate entry that described "possible Texas criminal history" and a recommendation for a follow-up search. The report listed an ex-boyfriend's address, even though she had never lived with the fellow. As MSNBC reporter Bob Sullivan writes, "The report also listed three automobiles she never owned and three companies listed that she never owned or worked for."

The report on the document provided to Deborah Pierce is very similar to an earlier report described by another privacy expert Richard Smith, "who paid a $20 fee and received a similar report from Choicepoint several years ago. The company offers a wide variety of reports on individuals; Smith purchased a commercial version that's sold to curious consumers. Smith's dossier had the same kind of errors that Pierce reported. His file also suggested a manual search of Texas court records was required, and listed him as connected to 30 businesses that he knew nothing about."

Third, Choicepoint and other information brokers have spent a great deal of time and money trying to block effective privacy legislation in Congress. According to disclosure forms filed with the U.S. House and Senate, obtained by the Wall Street Journal, Choicepoint and six of the country's other largest sellers of private consumer data spent at least $2.4 million last year to lobby members of Congress and a variety of federal agencies. The Journal reports that, "Choicepoint was the biggest spender, with $970,000 either paid to outside lobbyists or spent directly by the company."[12]

This improper disclosure and use of personal information is contributing to identity theft, which is today the number one crime in the United States. According to a 2003 survey by the Federal Trade Commission, over a one-year period nearly 5% of the adult populations were victims of some form of identity theft.[13]

EPIC'S EFFORTS TO BRING PUBLIC ATTENTION TO THE PROBLEMS WITH CHOICEPOINT

Well before the recent news of the Choicepoint debacle became public, EPIC had been pursuing the company and had written to the FTC to express deep concern about its business practices and its ability to flout the law. On December 16, 2004, EPIC urged the Federal Trade Commission to investigate Choicepoint and other data brokers for compliance with the Fair Credit Reporting Act (FCRA), the federal privacy law that helps insure that personal financial information is not used improperly.[14] The EPIC letter said that Choicepoint and its clients had performed an end-run around the FCRA and was selling personal information to law enforcement agencies, private investigators, and businesses without adequate privacy protection.

Choicepoint wrote back to us to say, in effect, that there was no problem The company claimed to fully comply with FCRA and that the question of whether FCRA, or other federal privacy laws, should apply to all of its products as simply a policy judgment. It made this claim at the same time it was spending several million dollars over the last few years to block the further expansion of the FCRA.

Mr. Chairman, hindsight may be 20-20, but it is remarkable to us that Choicepoint had the audacity to write such a letter when it already knew that state investigators had uncovered the fact that the company had sold information on American consumer to an identity theft ring. They were accusing us of inaccuracy at the same time that state and federal prosecutors knew that Choicepoint, *a company that offered services for business credentialing,* had exposed more than a hundred thousand Americans to a heightened risk of identity theft because it sold data to crooks.

But the problems with Choicepoint long preceded this recent episode. Thanks to Freedom of Information Act requests relentlessly pursued by EPIC's Senior Counsel Chris Hoofnagle, we have obtained over the last several yeas extraordinary documentation of Choicepoint's growing ties to federal agencies and the increasing concerns about the accuracy and legality of these products.[15] So far, EPIC has obtained FOIA documents from nine different agencies concerning Choicepoint. Much of the

---

[11] Bob Sullivan, "ChoicePoint files found riddled with errors Data broker offers no easy way to fix mistakes, either," MSNBC, March 8, 2005, *available at* http://www.msnbc.msn.com/id/7118767/.

[12] Evan Perez and Rick Brooks, "Data Providers Lobby to Block More Oversight," *Wall Street Journal,* March 4, 2005, at B1.

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

[14] Letter from Chris Jay Hoofnagle, Associate Director, EPIC, and Daniel J. Solove, Associate Professor, George Washington University Law School, to Federal Trade Commission, Dec. 16, 2004, *available at* http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[15] EPIC v. Dep't of Justice et al., No. 1:02cv0063 (CKK)(D.D.C.).

material is available on our web site at http:www.epic.org/privacy/Choicepoint. One document from the Department of Justice, dated December 13, 2002, discusses a "Report of Investigation and Misconduct Allegations . . . Concerning Unauthorized Disclosure of Information."[16] There are documents from the IRS that describe how the agency would mirror huge amounts of personal information on IRS computers so that Choicepoint could perform investigations.[17] Several documents describe Choicepoint's sole source contracts with such agencies as the United States Marshals Service and the FBI.[18]

Among the most significant documents obtained by EPIC were those from the Department of State, which revealed the growing conflicts between the United States and foreign governments that resulted from the efforts of Choicepoint to buy data on citizens across Latin America for use by the US federal law enforcement agencies.[19] One document lists news articles that were collected by the agency to track outrage in Mexico and other countries over the sale of personal information by Choicepoint.[20] A second document contains a cable from the American Embassy in Mexico to several different government agencies warning that a "potential firestorm may be brewing as a result of the sale of personal information by Choicepoint.[21] A third set of documents describes public relations strategies for the American Embassy to counter public anger surrounding the release of personal information of Latin Americans to Choicepoint.[22]

Choicepoint's activities have fueled opposition to the United States overseas and raised the alarming prospect that our country condones the violation of privacy laws of other government.[23] As USA Today reported on September 1, 2003:

> After the Mexican government complained that its federal voter rolls were the source, and were likely obtained illegally by a Mexican company that sold them to Choicepoint, the suburban Atlanta company cut off access to that information.
>
> In June, ChoicePoint wiped its hard drives of Mexicans' home addresses, passport numbers and even unlisted phone numbers. The company also backed out of Costa Rica and Argentina.
>
> ChoicePoint had been collecting personal information on residents of 10 Latin American countries—apparently without their consent or knowledge—allowing three dozen U.S. agencies to use it to track and arrest suspects inside and outside the United States.[24]
>
> The revelations helped kindle privacy movements in at least six countries where the company operates. Government officials have ordered—or threatened—inquiries into the data sales, saying ChoicePoint and the U.S. government violated national sovereignty.

LESSONS OF CHOICEPOINT

The Choicepoint incident proves many important lessons for the Congress as it considers how best to safeguard consumer privacy in the information age.

First, it should be clear now that privacy harms have real financial consequences. In considering privacy legislation in the past, Congress has often been reluctant to recognize the actual economic harm that consumers suffer when their personal information is misused, when inaccurate information leads to the loss of a loan, a job, or insurance. Consumers suffer harms both from information that is used for fraud and inaccurate information that leads to lost opportunities through no fault of the individual.

A clear example of how the company has contributed to the growing problem of identity theft may be found in Choicepoint's subscriber agreement for access to AutoTrackXP, a detailed dossier of individuals' personal information. A sample AutoTrackXP report on the ChoicePoint web site shows that it contains Social Security Numbers; driver license numbers; address history; phone numbers; property ownership and transfer records; vehicle, boat, and plane registrations; UCC filings; financial information such as bankruptcies, liens, and judgments; professional li-

---

[16] *Available at* http://www.epic.org/privacy/choicepoint/default.html.
[17] *Id.*
[18] *Id.*
[19] *Available at* http://www.epic.org/privacy/choicepoint/default.html.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] EPIC and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* 123-24, 182, 493 (2004) (Public Records, Argentina country report, Mexico country report)
[24] Associated Press, "Vendor sells Latin American citizen data to U.S.," Sept. 1, 2003, *available at* http://www.usatoday.com/tech/news/techpolicy/2003-09-01-choicepoint__x.htm.

censes; business affiliations; "other people who have used the same address of the subject," "possible licensed drivers at the subject's address," and information about the data subject's relatives and neighbors.[25] This sensitive information is available to a wide array of companies that do not need to articulate a specific need for personal information each time a report is purchased. Choicepoint's subscriber agreement shows that the company allows access to the following businesses: attorneys, law offices, investigations, banking, financial, retail, wholesale, insurance, human resources, security companies, process servers, news media, bail bonds, and if that isn't enough, Choicepoint also includes "other."

Second, it should be clear that market-based solutions fail utterly when there is no direct relationship between the consumer and the company that proposed to collect and sell information on the consumer. While we continue to believe that privacy legislation is also appropriate for routine business transactions, it should be obvious to even those that favor market-based solutions that this approach simply does not work where the consumer exercises no market control over the collection and use of their personal information. As computer security expert Bruce Schneier has noted, "ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security."[26] This argues strongly for regulation of the information broker industry.

Third, there are clearly problems with both the adequacy of protection under current federal law and the fact that many information products escape any kind privacy rules. Choicepoint has done a remarkable job of creating detailed profiles on American consumers that they believe are not subject to federal law. Products such as AutoTrackXP are as detailed as credit reports and have as much impact on opportunities in the marketplace for consumers as credit reports, yet Choicepoint has argued that they should not be subject to FCRA. Even their recent proposal to withdraw the sale of this information is not reassuring. They have left a significant loophole that will allow them to sell the data if they believe there is a consumer benefit.[27]

But even where legal coverage exists, there is insufficient enforcement, consumers find it difficult to exercise their rights, and the auditing is non-existent. According to EPIC's research, there is no indication that commercial data brokers audit their users and refer wrongdoers for prosecution. In other words, in the case where a legitimate company obtains personal information, there is no publicly available evidence that Choicepoint has any interest in whether that information is subsequently used for illegitimate purposes.

Law enforcement, which has developed increasingly close ties to information brokers such as Choicepoint seems to fall entirely outside of any auditing procedures. This is particularly troubling since even those reports that recommend greater law enforcement use of private sector databases for public safety recognize the importance of auditing to prevent abuse.[28]

And of course there are ongoing concerns about the broad permissible purposes under the FCRA, the use of credit header information to build detailed profiles, and the difficulty that consumers continue to face in trying to obtain free credit reports that they are entitled to under the FACTA.

Fourth, we believe this episode also demonstrates the failure of the FTC to aggressively pursue privacy protection. We have repeatedly urged the FTC to look into these matters. While on some occasions, the FTC has acted.[29] But too often the Commission has ignored privacy problems that are impacting consumer privacy and producing a loss of trust and confidence in the electronic marketplace. In the late 1990s, the FTC promoted self-regulation for the information broker industry and allowed a weak set of principles promulgated as the Individual References Service Group to take the place of effective legislation. It may well be that the Choicepoint fiasco could have been avoided if the Commission chose a different path when it considered the practices of the information broker industry.

---

[25] ChoicePoint, AutoTrackXP Report, http://www.choicepoint.com/sample__rpts/AutoTrackXP.pdf.

[26] "Schneier on Security: Choicepoint" *available at* http://www.schneier.com/blog/archives/2005/02/choicepoint.html.

[27] Aleksandra Todorova, "ChoicePoint to Restrict Sale of Personal Data," Smartmoney.com, March 4, 2005, *available at* http://www.smartmoney.com/bn/index.cfm?story=20050304015004.

[28] See Chris J. Hoofnagle, "Big Brother's Little Helpers: How Choicepoint and Other Commercial Data brokers Collect, process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation* (Summer 2004), *available at* http://ssrn.com/abstract=582302.

[29] *See* FTC's investigation into Microsoft's Passport program. Documentation *available at* http://www.epic.org/privacy/consumer/microsoft/passport.html.

The FTC has also failed to pursue claims that it could under section 5 of the FTC Act that prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumer nor offset by countervailing benefits to consumers and competition.[30] It may be that the unfairness doctrine could be applied in cases where there is no direct relationship between the consumer and the company, but to date the FTC has failed to do this.[31]

Fifth, we believe the Choicepoint episode makes clear the importance of state-based approaches to privacy protection. Congress simply should not pass laws that tie the hands of state legislators and prevent the development of innovative solutions that respond to emerging privacy concerns. Many states are today seeking to establish strong notification procedures to ensure that their residents are entitled to at least the same level of protection as was provided by California.[32]

In this particular case, the California notification statute helped ensure that consumers would at least be notified that they are at risk of heightened identity theft. This idea makes so much sense that 38 attorney generals wrote to Choicepoint to say that their residents should also be notified if their personal information was wrongly disclosed.[33] Choicepoint could not object. It was an obvious solution.

Finally, there is still a lot we do not know about the Choicepoint company. This firm has expanded so rapidly and acquired so many companies in the last few years, it is very difficult to assess how much information it actually has on Americans. As a starting point for further work by the Committee, I would urge you and Committee Staff to obtain your own Choicepoint records in the AutoTrackXP service as well as the National Comprehensive Report. This is the information about you that Choicepoint sells to strangers. If you want to understand the serious problem of record accuracy, this is one good place to start.

RECOMMENDATIONS

Clearly, there is a need for Congress to act. Although Choicepoint has taken some steps to address public concerns, it continues to take the position that it is fee to sell personal information on American consumers to whomever it wishes where Choicepoint, and not the consumer, believes there "consumer-driven benefit or transaction."[34] Moreover, the company remains free to change its policies at some point in the future, and the steps taken to date do not address the larger concerns across the information broker industry.

Modest proposals such as the extension of the Gramm-Leach-Bliley Act's Security Safeguards Rule are unlikely to prevent future Choicepoint debacles. The Safeguards Rule merely requires that financial institutions have reasonable policies and procedures to ensure the security and confidentiality of customer information. Recall that the disclosure by Choicepoint did not result from a "hack" or a "theft" but from a routine sale. Moreover, the Security Safeguards Rule will do nothing to give consumers greater control over the transfer of their personal information to third parties or to promote record accuracy.

Extending notification statutes such as the California bill would be a sensible step but this is only a partial answer. Notification only addresses the problem once the disclosure has occurred. The goal should be to minimize the likelihood of future disclosure. It is also important to ensure that any federal notification bill is as least as good as the California state bill and leaves the states the freedom to develop stronger and more effective measures. What happens for example, when at some point in the future, we must contend with the extraordinary privacy problems that

---

[30] 15 U.S.C. 45(n); Letter from Michael Pertschuk, FTC Chairman, and Paul Rand Dixon, FTC Commissioner, to Wendell H. Ford, Chairman, House Commerce Subcommittee on Commerce, Science, and Transportation (Dec. 17, 1980), at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[31] In *FTC v. Rapp,* the "Touch Tone" case, the FTC pursued private investigators engaged in "pretexting," a practice where an individual requests personal information about others under false pretenses. No. 99-WM-783 (D. Colo. 2000), 2000 U.S. Dist. LEXIS 20627. In a typical scheme, the investigator will call a bank with another's Social Security Number, claim that he has forgotten his bank balances, and requests that the information be given over the phone. The FTC alleged that this practice of the defendants, was deceptive and unfair. It was deceptive because the defendants deceived the bank in providing the personal information of another. The practice was unfair in that it occurs without the knowledge or consent of the individual, and it is unreasonably difficult to avoid being victimized by the practice.

[32] "Choicepoint Incident Prompts State Lawmakers to Offer Data Notification Bills," 10 *BNA Electronic Commerce & Law Report* 217-18 (March 9, 2005)

[33] Associated Press, "38 AGs send open letter to ChoicePoint," *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint_x.htm.

[34] "Choicepoint Halts Sale of Sensitive Information, as Agencies Launch Probes," 10 *BNA Electronic Commerce and Law Report* 219 (March 9, 2005).

will result from the disclosure of personal information contained in a database built on biometric identifiers?

At this time, legislation such as the Information Protection and Security Act, H.R. 1080, provides a good starting point to safeguard consumer privacy and reduce the growing threat of identity theft. It would allow the FTC to develop fair information practices for data brokers; violators would be subject to civil penalties. Enforcement authority would be given to the FTC and state attorneys general. Consumers would be able to pursue a private right of action, albeit a modest one. And states would be free to develop stronger measures if they chose.

But a stronger measure would establish by statute these same authorities and impose stricter reporting requirements on the information broker industry. It would include a liquidated damages provision that sets a floor, not a limit, on damages when a violation occurs, as is found in other privacy laws. It is even conceivable that Congress could mandate that information brokers provide to consumers the same information that they propose to sell to a third party prior to the sale. This would make consent meaningful. It would promote record accuracy. And it would allow the consumer to determine for himself or herself whether in fact the transaction will provide a "consumer-driven benefit." Proposals for credit report "freeze" legislation that allow consumers to determine when it is in their benefit to release personal credit information provides a good parallel for strong legislation in the data broker field.

Furthermore, to the extent that information brokers, such as Choicepoint, routinely sell data to law enforcement and other federal agencies, they should be subject to the federal Privacy Act. A "privatized intelligence service," as Washington Post reporter Robert O'Harrow has aptly described the company, Choicepoint should not be permitted to flout the legal rules that help ensure accuracy, accountability, and due process in the use of personal information by federal agencies.[35]

Also, a very good framework has been put forward by Professor Daniel Solove and EPIC's Chris Hoofnagle.[36] This approach is similar to other frameworks that attempt to articulate Fair Information Practices in the collection and use of personal information. But Solove and Hoofnagle make a further point that is particularly important in the context of this hearing today on Choicepoint. Increasingly, the personal information made available through public records to enable oversight of government records has been transformed into a privatized commodity that does little to further government oversight but does much to undermine the freedom of Americans. While EPIC continues to favor strong open government laws, it is clearly the case that open government interests are not served when the government compels the production of personal information, sells the information to private data vendors, who then make detailed profiles available to strangers. This is a perversion of the purpose of public records.

Looking ahead, there is a very real risk that the consequences of improper data use and data disclosure are likely to accelerate in the years ahead. One has only to look at the sharp increase in identity theft documented by the Federal Trade Commission, consider the extraordinary rate of data aggregation in new digital environments, as well as the enormous efforts of the federal government to build ever more elaborate databases to realize that the risk to personal privacy is increasing rapidly. Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-terms solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguard privacy.

Congress needs to establish a comprehensive framework to safeguard the right of privacy in the twenty-first century. With identity theft already the number one crime, and the recent spate of disclosures, any further delay could come at enormous cost to American consumers and the American economy.

Finally, Mr. Chairman, there are several practical questions left open by the Choicepoint matter. First, as we said to the FTC in December, Choicepoint has done a poor job tracking he use of personal information on American consumers that it routinely sells to strangers. Now is the time for Choicepoint to go back to its audit logs and determine what the legal basis was for selling the information that was

---

[35] Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press 2005).

[36] Daniel Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection," March 8, 2005, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902.

provided to the identity theft ring. In fact, we believe that Choicepoint should be required to review all of its audit logs for the past year and report to this committee on whether it has uncovered any other instance of breaches within the company. Just as heads of financial companies are now required to vouch for the accuracy of their financial statements, the heads of the information broker companies should be required to make an annual representation tot he public that they have reviewed the audit logs of their companies and are assured that the information they have disclosed has only been used for lawful purposes.

Second, there is the question of what Choicepoint intends to do with the money that it received from the sale of personal information to an identity theft ring. How can Choicepoint possibly keep the funds from those transactions? In a letter that EPIC sent to Choicepoint COO Douglas Curling, we urged the company to "disgorge the funds that you obtained from the sale of the data and make these funds available to the individuals who will suffer from identity theft as a result of this disclosure." Since Mr. Smith, the company's President is at the hearing today, perhaps he can explain what Choicepoint will do with the funds.

Third Choicepoint has still not provided to the victims of the negligent sale the same information that it disclosed to the identity thieves. At the very least, we think the company should give people the same records it sold to the crooks.

CONCLUSION

For many years, privacy laws came up either because of the efforts of a forward-looking Congress or the tragic experience of a few individuals. Now we are entering a new era. Privacy is no longer theoretical. It is no longer about the video records of a federal judge or the driver registry information of a young actress. Today privacy violations affect hundreds of thousands of American all across the country. The harm is real and the consequences are devastating.

Whatever one's view may be of the best general approach to privacy protection, there is no meaningful way that market-based solutions can protect the privacy of American consumers when consumers have no direct dealings with the companies that collect and sell their personal information. There is too much secrecy, too little accountability, and too much risk of far-reaching economic damage. The Choicepoint debacle has made this clear.

The Committee may not be able to solve every privacy problem, but I urge you today to focus on the information broker industry and to pass legislation such as the Information Protection and Security Act. The information broker industry has been flying under the radar for too long.

I appreciate the opportunity to be here today. I will be pleased to answer your questions

REFERENCES

EPIC Choicepoint Page, available at http://www.epic.org/privacy/choicepoint/

Mr. STEARNS. I thank the gentleman, and I will start the questions. Just the two of us. Mr. Rotenberg, I think you are saying that ChoicePoint, in your opinion, violated the Fair Credit Reporting Act. Is that true?

Mr. ROTENBERG. Well, it is not clear to us, sir, at this point, if we can say that, because we don't know exactly what type of information was disclosed, and if it was subject to the Fair Credit Reporting Act.

Mr. STEARNS. But you are saying that, you know, that you thought the products and service they are providing, they provided something so they wouldn't have to comply, so they just tweaked a bit, tailored a bit, so that they could avoid oversight that you feel is critical to the consumer, and would have the applicability of the Fair Credit Reporting Act.

Mr. ROTENBERG. Yes.

Mr. STEARNS. So you are sort of—you are suggesting that they did this so that they wouldn't have to comply, so the question is, you can't really say whether they violated it at this point, only because you don't know—you are asking the FTC to tell us, right?

Mr. ROTENBERG. Right.

Mr. STEARNS. Yes.

Mr. ROTENBERG. Well, we did say in our letter that we believe that a particular product, the AutoTrack XP product, which contains a great deal of detailed personal information on American consumers, much like a credit report does, should be subject to rules like the Fair Credit Reporting Act. Now, ChoicePoint has taken the position that that product is not subject to the Fair Credit Reporting Act.

Mr. STEARNS. It is called Auto——

Mr. ROTENBERG. AutoTrack XP.

Mr. STEARNS. XP. Gee, I don't think many people, Members of Congress——

Mr. ROTENBERG. No, I don't think so.

Mr. STEARNS. [continuing] know anything about the AutoTrack—so it is pretty much like a consumer report.

Mr. ROTENBERG. Yes, that is our view.

Mr. STEARNS. Yeah, and they are—they don't think it is.

Mr. ROTENBERG. No. In fact, we had an exchange of letters with them when we filed our complaint at the Federal Trade Commission, I heard from Mr. Curling, who is their Chief Operating Officer, and he said that their company had simply taken the position that this product was not subject to the FCRA. He——

Mr. STEARNS. Is the AutoTrack XP, still—are they still doing it? Is ChoicePoint——

Mr. ROTENBERG. This is the interesting question that is raised by the hearing today, because Mr. Smith suggested that ChoicePoint was withdrawing from the non-FCRA products.

Mr. STEARNS. Okay. So doesn't——

Mr. ROTENBERG. But then, he left——

Mr. STEARNS. [continuing] the withdrawal now, that attention has been called.

Mr. ROTENBERG. That is right. But he left significant loopholes.

Mr. STEARNS. Yeah.

Mr. ROTENBERG. And he said for example, products that might provide a consumer benefit, they would continue with. So it is, I think an open question at this point, what they plan to do with this particular product.

Mr. STEARNS. Mr. Ansanelli, you have software, is that what you have, is your company providing software? Is that primary—your product?

Mr. ANSANELLI. That is correct. We provide software for information security.

Mr. STEARNS. And do you work with ChoicePoint, or do you work with LexisNexis at all?

Mr. ANSANELLI. Currently, neither of those are customers of ours now.

Mr. STEARNS. Tell me some of your customers.

Mr. ANSANELLI. Companies like Prudential Financial, Best Buy, Charles Schwab, basically a lot of companies that store lots of consumer data, and want to make sure that it doesn't get out inappropriately over the Internet.

Mr. STEARNS. Do you feel—you have heard most of the testimony today—do you feel that we need Federal legislation, as Mr. Rotenberg has talked about?

Mr. ANSANELLI. I think there has been a discussion about two parts of Federal legislation, both security and privacy. I am a little bit more knowledgeable on the security side, and I would——

Mr. STEARNS. Right.

Mr. ANSANELLI. [continuing] say that things like Gramm-Leach-Bliley, in financial services, have made an impact in terms of the data at banks and other financial institutions being more secure, and I do think it is a question why, when the similar data is stored by other organizations that might not be in financial services, like a Social Security number, or a credit card, why that data does not have to be protected in the same way we require a bank or a financial institution. And I think that in order to ever get to a state where we have improved privacy, you must first have security, so that is why we do suggest that some improvements in clarifying what the requirements are for data security, regardless of the industry, would make a big difference.

Mr. STEARNS. When I was talking to Mr. Sanford, he didn't quite understand my question. Maybe outsourcing was not the right word, but I was saying that if you had a company, and you bought me, as another company, and then I had employees that had access to all these passwords right on up the line, how do you have the assurance that the password he has, he works for me, he is not using that for his own personal use? So how does a CEO, in this case, of LexisNexis, control the company they bought's employees, who have access to, all up the line, the passwords? And that is why I started to go—I mean, how would you suggest we control the security on that?

Mr. ANSANELLI. I think you are commenting on something many people refer to as the insider security threat.

Mr. STEARNS. Yeah, insider. That is better than outsourcing. That is why—he didn't quite—that is what I mean, insider security threat.

Mr. ANSANELLI. And it is obviously quite complicated.

Mr. STEARNS. Yeah.

Mr. ANSANELLI. Most security and infrastructure has focused on the issue of hackers trying to break into networks, and trying to get access to data, where many of the very known cases are actually issues of people with legitimate, allegedly legitimate credentials, either by borrowing a password, or stealing a password, gaining access to information.

Mr. STEARNS. But you could include the customers, not just the employees, too.

Mr. ANSANELLI. Correct. I mean——

Mr. STEARNS. So you have not only the insider trading, but you have customers having this access.

Mr. ANSANELLI. Correct. I mean, the case at AOL, it is alleged that there was an IT professional who stole all the email addresses at AOL, because he borrowed a password from somebody else and got access to that data base. A number of things that people can do. Clearly, you know, one of the things is clearly what we do, which is monitoring to make sure that the data is not getting out.

So for example, if someone gets access to that data that shouldn't be sending it, either via email or over the Web, we can help organizations to understand when information like Social Security numbers or credit card numbers are being distributed inappropriately electronically, outside the company. That is clearly an important thing that many, many companies are starting to do.

There is also—there is important things in terms of sort of physical precautions. How do you limit——

Mr. STEARNS. You change the passwords frequently.

Mr. ANSANELLI. Changing passwords frequently, making sure that the—there is also technologies which allow for stronger things than just a password and a name. You might have to actually have a physical card that has an identifier which is constantly changing, for example. So there is many, many things that people can do, and you know, one thing I would say, though, is I think it is important that legislation not recommend any particular technology.

Mr. STEARNS. No, no. I understand. It is just that——

Mr. ANSANELLI. There is lots going——

Mr. STEARNS. My time has expired. Mr. Rotenberg, when I had the discussion with the CEOs, I sort of alluded to the fact there might be a third party required to authenticate their—that their system is secure, or that they are—have best practices. And I don't think they want that. Do you think that is something that is necessary? I mean, like, to verify that the corporations P&L, they have an outside accounting firm. And he—the accounting firm authenticates, and if it turns out, like in the case of Enron, in which—and that accounting firm shows a lack of credibility, and they lose their business. So it is to the advantage of the accounting firm, just like it would be to the security firm, to say this company is secure, and is doing best practices.

I don't know. Is that——

Mr. ROTENBERG. I think that is a very good proposal, Mr. Chairman. In fact, when we wrote to the FTC in December, one of the issues that we raised with them was the lack of auditing. You know, under the FCRA, people get information for permissible purposes, but very little effort is made after the information is disclosed, to determine if, in fact, the information was used for a permissible purpose. And we think systems of better auditing and outside auditing would reduce the likelihood of the misuse of information, and I think it would make the companies more accountable.

Mr. STEARNS. I mean, just the fact if you kept a data base of companies that have breaks in security, and you pretty soon knew which companies did and which didn't, and it started to be a reoccurring pattern, that would be something that would be very helpful to alert the Federal Trade Commission and everybody else, hey, there is a problem here with our security. Just the reporting process.

Mr. ROTENBERG. Yeah, I think it is a very good proposal, and I think also for the CEO to certify the adequacy of the auditing, the accounting of this personal information, would serve much of the same purpose that was done when concerns were raised about financial reporting, and the risks to consumers are very similar. When mistakes are made, consumers carry those costs.

Mr. STEARNS. Well, obviously, you could do this voluntarily through a best practice association that does this for them, but it seems to me, in the case of ChoicePoint, this individual in Los Angeles, they did everything, yet the individual was using it fraudulently, and there is nothing they could have done about it.

My time has expired. Ms. Schakowsky.

Ms. SCHAKOWSKY. You know, Mr. Chairman, there actually was a report issued. I don't know much about—the Ponemon, Ponemon Institute, of 163 U.S. companies that were surveyed in the past 12 months, 75 percent reported a serious security breach resulting in stolen data, and of those breaches, 27 percent involved customer information.

I mean, we haven't heard reports about that. I am wondering, is this because there is unwillingness to make the investment, because they don't know best practices, because we have failed to make requirements on them to implement certain practices? Mr. Ansanelli?

Mr. ANSANELLI. I do think that one of the issues is clear requirements for organizations that store data. I mean, financial services organizations under GLBA clearly now, and have a requirement, and guidelines both by the FTC, as well as the financial services agencies, to what they are supposed to do. But other companies in different industries that have similar data don't have the same requirements. So without clear requirements, with respect to protecting the data, as well as notification, I don't think it should be too much of a surprise that necessarily people haven't come forward with it.

I do think that one of the other challenges and issues is that there is a concern that if companies are proactive in doing things, that they are taking on additional litigation risk, that people are going to sue them for punitive damages, and that has definitely been something which, I think, presents a bit of a stumbling block for some companies, that I suggest we can deal with as well.

Ms. SCHAKOWSKY. To both of you. A few—California and a few other States have laws that allow consumers to put security freezes on their credit reports, and the freezes mean that their credit reports can't be accessed, unless the consumer allows it to be accessed, an opt-in. Do you think laws of this type would be useful for other personal information that is held by data brokers? Mr. Rotenberg.

Mr. ROTENBERG. I think it is a very sensible proposal. I mean, all of us understand that this disclosure of personal information will, in some circumstances, provide important benefits to consumers, to obtain a loan or, you know, a job, or some of these other things. But if there is a benefit to the consumer, it would seem obvious that the consumer should be able to decide when the information is disclosed. And what consumer organizations have realized over the last couple of years is that if we simply say, if you are intending to get a home loan, for example, at that point, you will make your credit report available, and others can make use of it, and make a determination, and if you are not intending to get a loan, or there is no other basis for someone to get access to your credit report, then it really should be in the offsetting.

So that particular approach, which both recognizes that this information is important to businesses making decisions about consumers, and gives consumers control over the disclosure of the information, I think is absolutely the right approach. I hope we will follow it in more areas.

Ms. SCHAKOWSKY. Thank you. I wanted to follow up on this issue of victims of domestic violence, where it didn't sound like—well, at least off the top of their head, that either company was aware of the kind of procedures that may be put in place.

Is this a problem, and is there an obvious solution to that problem, where even an address could put someone's life in jeopardy?

Mr. ROTENBERG. Congresswoman, I am not certain about the specific practices of the information broker industry today. I can tell you that in the privacy world, we confronted a very similar issue more than 15 years ago, when Caller ID first became available, and you know, and people who were in shelters and elsewhere were very concerned about their ability to make contact with family members, without having their location or actual phone number disclosed, and at that time, when we were arguing for privacy protection as Caller ID was being introduced, the telephone companies agreed to put in place what was called per line blocking, so that people calling from shelters would not have their numbers disclosed, and they wouldn't even have to worry about it.

I think today, you know, to do at least something like that, in the information broker industry, should be expected.

Ms. SCHAKOWSKY. You know, the fact that these data brokers are required, under—to have certain data under the Fair Credit Reporting Act, under Gramm-Leach-Bliley, under all those protection, the usefulness of that fact is dependent on anybody knowing about it. I mean, I have been asking all the witnesses who the heck knew before the ChoicePoint scandal came out really, that these companies even really existed? I mean, in terms of mass knowledge of this, I think it was nonexistent.

So is this really useful, that they have to comply, and they have to provide information back to consumers, if nobody knows about it, and what are we going to do about that?

Mr. ROTENBERG. Well, as I tried to explain in my testimony, I think the absence of the relationship between the consumer and the business makes clear that market-based solutions simply can't work. I mean, you have to regulate in this area, because there is no other effective mechanism, and in fact, this was exactly the same theory that the Congress pursued, leading up to the passage of the Fair Credit Reporting Act in 1970. And the Congress looked at it, and they said well, this information is being compiled on American consumers. They are not going to have a choice over which credit reporting agency is going to collect and use this information, so it has to be regulated, and you have to do what you can to minimize the misuse of this information, which continues to be a problem as well.

Ms. SCHAKOWSKY. I would agree with that. Do you want to——

Mr. ANSANELLI. I think the one thing I would add is again, with respect to ID theft, I do think that consumer education is really, really important, and I do think that the FTC has done a fair amount in that area, and I think they continue to do more, in

terms of people just not understanding what is going on. There is no—there is very—there is not an obvious place where they go right now to get that information about where their data is, and how they can deal with it, and I do think more can be done there.

Ms. SCHAKOWSKY. That is true, but I think that putting the onus on the consumer is ultimately a problem, because I think there are so many actors in this field that you could spend your life trying to get that information, and make sure that you are protected. I think we do have a role here.

Mr. ANSANELLI. I would agree. I wasn't suggesting that would be the only thing. I do think that there are those three areas, again, the criminals, the companies, and the consumers all play a role in this, and I think we could do more on all three of those efforts.

Ms. SCHAKOWSKY. Thank you very much.

Mr. STEARNS. Well, I want to thank you for staying with us all through this roughly 4 hours, and your contribution is very helpful, and I think it is nice to have a little bit of a different slant.

So we are going to conclude the hearing. I think it has been very productive, and I want to thank you again for waiting for the other two panels.

And with that, the committee is adjourned.

[Whereupon, at 2 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

Questions for Mr. Derek Smith, Chairman and CEO, ChoicePoint Inc.
Subcommittee on Commerce, Trade and Consumer Protection Hearing
"Protecting Consumer Data: Policy Issue Raised by ChoicePoint"
March 15, 2005

The Honorable John D. Dingell

1. Your written testimony of March 15, 2005, pages (2-3) stated that:

"We have decided to exit the consumer sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will no longer sell information products containing sensitive consumer data including social security and drivers license numbers except where there is a specific consumer driven transaction or benefit or where the products support federal, state or local government and criminal justice purposes."

a. Please list and describe what products and/or customers ChoicePoint intends to eliminate, and any other product modifications that may be planned.

ChoicePoint has decided to discontinue the sale of information products that contain personally identifiable information unless those products and services meet one of three tests:

1. ***The product supports consumer driven transactions such as insurance, employment and tenant screening, or provides consumers with access to their own data;***
2. ***The product provides authentication or fraud prevention tools to large accredited corporate customers where consumers have existing relationships; or***
3. ***When personally identifiable information is needed to assist federal, state or local government and criminal justice agencies in their important missions.***

As part of this process, we modified certain products to eliminate the delivery of full social security numbers to certain markets.

b. Describe and provide specific examples of consumer-driven transactions or benefits. Do unsolicited credit card applications sent to targeted consumers through the mail or on the Internet provide a "consumer benefit"? Do you also consider costs or downsides such as facilitation of identity theft and fraud?

Examples of consumer-driven transactions or benefits would include the purchase of auto or homeowners insurance, as well as employment and tenant screening. As a point of clarification, ChoicePoint's direct marketing services do not entail the disclosure of personally identifiable information (i.e., social security numbers or drivers licenses.)

2. Your written testimony of March 15, 2005, further stated at page 3 that: "We have strengthened ChoicePoint's customer credentialing process and we are changing our

products and services to many customer segments." Please describe the specific changes that ChoicePoint has made.

We are requiring more stringent due diligence such as bank references and site visits before allowing businesses access to personally identifiable information. We are also re-credentialing broad sections of our customer base, including our small business customers.

We have decided to centralized the credentialing processes for all business units that have products and services that include personally identifiable information. In addition, we have created an independent office of Credentialing, Compliance and Privacy that will ultimately report to our Board of Directors' Privacy Committee. This office will be led by Carol DiBattiste, the former deputy administrator of the Transportation Security Administration and a former senior prosecutor in the Department of Justice with extensive experience in the detection and prosecution of financial fraud.

Finally, we have appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the federal government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials. In this role, he will work aggressively to ensure that criminal activities are investigated and prosecuted to the fullest extent possible. He will also help us ensure that our security and safeguards procedures continue to evolve and improve.

3. A March 8, 2005 MSNBC report, "ChoicePoint files found riddled with errors: Data broker offers no easy way to fix mistakes, either" (copy attached), reveals that a person who had never been in any legal trouble had the notation "possible Texas criminal history" in her file. An entry like this could cause enormous harm to a person.

a. Please explain under what circumstances ChoicePoint would add the negative notation "possible criminal history" to an individual's file. Is it a public record? Was it taken from a public record? Is it a judgment made by ChoicePoint or its agent?

It is important to note that a product delivered is a result of the search input criteria. Our customers may start with a search that is not related to a specific individual. As such, the results of the searches may include records associated with many individuals at a particular address. Additionally, the results of the searches are dependent upon the data types that are searched and the point in time that the search was made.

The attached report contains an example of a "possible criminal history" This is the result of a specific search on "Zach Thul". This investigative report is designed to provide potential matches for further research by the report requestor. These matches are made from public records provided to ChoicePoint by various state agencies. As discussed further in Question 3d, the use of the term "possible" does not reflect a judgment but rather the lack of identifiers and the ability to validate a match with the record and the individual.

ChoicePoint provides the following disclaimer on all criminal searches and reports returned through Public Filings Applications:

THIS INFORMATION IS NOT TO BE USED FOR PREEMPLOYMENT PURPOSES. As this INFORMATION is compiled from individual sources, ChoicePoint Public Records Inc. does not warrant the accuracy or comprehensiveness of these records. This may or may not be a complete criminal and/or civil history. The data indicates a possible criminal and/or civil history on the searched subject; however a full file should be pulled directly from the agency to confirm the proper identity of the subject and any additional information available

b. If someone is denied a job or a security clearance based on such a notation, and that person has no criminal record, who is liable for the damage caused by losing a job or security clearance or the damage to the person's reputation?

Pre-employment screening is conducted pursuant to the Fair Credit Reporting Act. Accordingly, in the event that a report results in derogatory information, the applicant would have the right to review and dispute that information. In addition, our Subscriber agreement specifically prohibits our customers from rendering an employment judgment based on the public records information contained in such a report.

Screening by ChoicePoint for security clearance purposes is performed as a pre-employment process and is governed by the FCRA. It is possible that a government agency may use a public record report for investigative processes and tip and lead information but not for a clearance determination.

c. The MSNBC report indicates that the criminal-history notation was included in a document called a "National Comprehensive Report." Please describe this report in detail and to whom it may be sold.

The National Comprehensive Report is an investigative report that is designed to provide "tip and lead" information for further resolution by an investigator. It is not sold for use in pre-employment screening nor is an investigator to rely solely upon the information provided in the report as was explained more thoroughly in our response to Question 3b. A sample report is also attached.

d. There were numerous other errors in this report. Is the National Comprehensive Report a product that an individual consumer would be aware of? If so, how? If there were errors in this report, how would the consumer correct those errors?

Unfortunately, public filings are not perfect and to the extent errors are included in the information provided to us by issuing agencies, it is possible we may pass this erroneous information on to our subscribers.

Because issuing agencies have restricted their use of clear identifiers (SSN/DOB/Address), the likelihood that a valid match will be made to an incorrect

subject has increased (i.e., is this John Smith MY John Smith?) Accordingly, use of the term "possible" is used to differentiate the strength of the match. As mentioned above, when link data like SSN/Address/DOB is not present, the link to a business or a derogatory record could be made but will be marked as "possible".

e. According to this same MSNBC report, a person that ChoicePoint contacted in February because her name was one of the 145,000 whose information may have been compromised received her "public records" file and found it full of errors. She was tied to businesses that she knew nothing about, apparently because a post office box number she once had was associated with at least some of these businesses. She was named as the officer of a firm she had never heard of. When she asked ChoicePoint how to fix these errors, she was told to contact the source of ChoicePoint's information. Is it ChoicePoint's position that it has a right to make money by collecting information about people and selling it, but it has no obligation to make sure that the information is correct?

If a consumer is adversely impacted by information contained in one of our products governed by the FCRA, she would have the ability to contest that information through ChoicePoint. However, to dispute information contained in public records, ChoicePoint's policy is to direct the consumer to the source of the data. The logic behind that decision was three-fold:

1. As a data aggregator, we do not feel qualified to judge the accuracy of the exception lodged by the customer. (i.e., we don't know if a tax lien is accurate or not)

2. Were we to expunge or modify our record without the "source" making a change, there is a strong likelihood that a subsequent update from the source would overwrite our change.

3. Were we to expunge or modify our record without the "source" making a change, the potentially erroneous record would continue to propagate thru other means.

If a correction is made by the "source", ChoicePoint will update any data that we maintain to reflect that correction as well.

4. Consumers are allowed to put a fraud alert on their credit bureau files when they believe that their information may have been compromised. Do you think that consumers should be able to place a "contested information" alert on their files, including those originating from ChoicePoint, to attempt to correct the information? Why or why not?

ChoicePoint believes that consumers should have the ability to put fraud alerts on their files. In response to the recent incident in California, we considered adding alerts to the files of affected consumers. However, we ultimately decided that such a decision was best left to consumers as the alerts might make it more difficult and/or more expensive for consumers to obtain credit. Accordingly, we advised affected consumers

regarding the availability of these alerts and provided them with a single point of contact for requesting such an alert.

Moreover, ChoicePoint supports the ability of consumers to insert a comment on their records. In my letter to shareholders in the 2003 Annual Report, I stated "[e]veryone should have the right of access to information about them, irrespective of the type, source or use of the information. In other words, extend the principles of the Fair Credit Reporting Act to all types of information: right of access, right to question the accuracy and a prompt review, and the right to comment if a negative record is found to be accurate."

5. Consumers currently have no legal right to review the information that data brokers hold beyond that contained in their credit reports. Should consumers have the right to see what ChoicePoint and other data brokers have in all of their files and to make corrections if information is incorrect?

See response to Question 4.

6. In 2002, one of ChoicePoint's subsidiaries provided incorrect information about whether certain Florida voters were convicted felons, which points to significant weaknesses in your criminal databases. It resulted in the improper disenfranchisement of approximately 1,000 voters. What steps has the company taken to assure more accurate information and to identify the actual persons who were convicted felons? Did this database also contain the notation "possible criminal history"?

ChoicePoint has never been involved in the review of voter registration rolls in Florida or any other state, and has no plans to do so in the future. Rather, ChoicePoint acquired the company in May 2000 that did – Database Technologies – after DBT had delivered the initial 2000 voter exception list to Florida officials for verification.

7. Anyone who has been the victim of identity theft knows that negative information can show up again and again over several years, even after it seemed to have been corrected. Why is ChoicePoint providing credit report monitoring for only one year? If the misinformation keeps showing up or identity thefts continue beyond one year, what additional assistance do you intend to provide to affected consumers?

ChoicePoint has voluntarily taken a number of steps to help assist and protect consumers who may have been harmed. In addition to providing, free of charge, a one year subscription to a credit monitoring service, the Company has arranged for a dedicated web site and toll-free number and is also providing a free 3-bureau credit report for affected consumers. We are also arranging for support services to be provided to actual victims of identity theft through a $1 million grant to the Identity Theft Resource Center located in San Diego, California. The Center will provide counseling services as well as consumer education and awareness and best practices surrounding identity theft and personal privacy. We will continue to evaluate the situation and will take additional measures if future conditions warrant.

8. Under current practice, could an individual request all of the information that ChoicePoint had collected on them? How much would those reports cost?

A consumer may access his or her report through ChoiceTrust.com. A consumer may access this report for free once annually.

9. Recently, there has been discussion of using truncated Social Security numbers for customers who have little or no need for that information. What is your position on the use of truncation?

As noted during testimony, ChoicePoint supports efforts to restrict the use and, in particular, the display of social security numbers. Truncation of social security numbers would be one way to preserve the means of identifying an individual. However, ChoicePoint does not support a blanket prohibition on the display of full social security numbers as it would impair legitimate law enforcement and fraud prevention activities.

Social Security numbers and other personally identifiable information is critical to many commercial and government entities to ensure the information provided is associated with the proper individual. As such, a blanket prohibition would have negative implications.

10. The European Data Protection Directive, implemented in 1998, gives people the right to access their information, correct inaccuracies, and deny permission for it to be shared. Moreover, it places the cost of mistakes on the companies that collect the data and not on the harmed individuals. What are your views on this framework?

ChoicePoint supports a consumer's right to access his/her records. Moreover, we support a process where the consumer has a right to go to the originator of the record and request correction- if such a correction is made by the source, we would make the change as well (see the answer to Question 3e above)

ChoicePoint does not support the denial of permission for the following reasons-

- ***As public records, significant thought has already been given by elected representatives and consumers that there is a valuable public interest served in making the records available***
- ***An opt out would allow a fraudster to remove themselves, and evidence of their fraudulent behavior, from public scrutiny.***
- ***Aggregation of this data and the ability to search it provides a valuable public good- both from a public perspective (e.g., law enforcement, public safety, credentialing, fraud prevention) and in the private sector (security, anti-fraud, etc)***
- ***Current laws already provide for court remedies where actual harm has occurred.***

11. In the past seven years, how many security breaches involving the information of more than 100 consumers has ChoicePoint had? Please describe these breaches and indicate

whether your company notified consumers and, if so, how long after the company was made aware of the problem. If not, what steps were taken?

The FTC is conducting a preliminary inquiry that focuses on many of these issues. Once these inquiries are completed, we will be in a better position to respond to the specifics of your question. However, we are aware of other breaches and our internal investigation identified between 45-50 accounts that we determined were fraudulent. Consumers whose information may have been accessed through these accounts have been notified.

Additionally, we found an account recently that we have investigated and identified approximately 100 consumers whom we have now identified.

a. When did you first learn about the most recent compromise of your database? Who provided this information to you? In October of 2004, who was the highest-level ChoicePoint official aware of the breach? Please describe the internal notification process that your company has in place for notification of senior management when significant security breaches occur, and any changes that have been made in that process since October of 2004.

In addition, the FTC and the SEC are conducting preliminary inquiries that focus on many of these issues. Once these inquiries are completed, we will be in a better position to respond to the specifics of your question.

With respect to the final part of this question, as I stated in my testimony, in the future, I will be notified when ChoicePoint learns of a formal law enforcement inquiry involving any potential breach of our security.

b. Serious concerns have been raised about the length of time that ChoicePoint delayed notifying affected consumers that their information may have been compromised. It appears that the company learned about the breach at the end of September in 2004, but it did not inform consumers until mid-February of 2005. At a meeting with Committee staff, company representatives laid the blame at the feet of law enforcement officials. But according to a March 5, 2005 **New York Times** article, "Release of Consumers' Data Spurs ChoicePoint Inquiries," the Southern California Identity Theft Task Force asked the company on November 23, 2004, to delay notifying consumers for 30 days. What was the reason for the additional delay?

The California notification statute authorizes law enforcement officials to delay notification to allow a criminal investigation to proceed. Last fall, ChoicePoint received such a request from the Sheriff's Department after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time ChoicePoint had not yet reconstructed all of the searches required to identify consumers at risk and law enforcement officers had not yet learned all of the pertinent details of the crime. Working cooperatively with the Sheriff's Department and after completing the necessary reconstruction, we began the process of notifying consumers in February.

c. Why did ChoicePoint initially tell the public that the 2004 breach was the first such compromise of its databases when a similar breach had occurred in 2000, and one of the perpetrators received a jail term in 2002? In that case, press reports indicate that two people used a fake real estate broker's license and a stolen Social Security number to open an account with ChoicePoint and steal $1 million.

As part of our investigation resulting from the 2004 Los Angeles incident and utilizing what we learned about the criminal methodology, we began a review of other accounts and historical contacts with law enforcement on fraud incidents or other related matters including subpoenas. Our mailing earlier this year to approximately 145,000 potentially affected consumers included all the customer accounts we were able to identify during this investigation.

d. Did ChoicePoint take any steps to improve security after that incident? If so, please describe those changes. Why did those security enhancements fail in 2004?

See response to Question 2..

12. What steps, if any, does ChoicePoint take to assure that your customers have appropriate security in place to protect the information that ChoicePoint provides them?

We contractually require our customers to comply with applicable federal and state laws that govern the physical security of information. This issue is among those that the Carol DiBatiste, the newly appointed Director of the Office of Credentialing, Compliance and Privacy, will review.

13. Concerns have been raised that ChoicePoint placed too much emphasis on growing its business and too little emphasis on safeguarding the personal information that it collects and disseminates and ensuring its accuracy. Please list all of the businesses that ChoicePoint has acquired from 2000 to the present. Please describe the enhancements to internal controls and safeguards that were made by your company in each case to ensure that accurate information was being collected and disseminated and that personal information would not be compromised.

ChoicePoint understands the importance of protecting the data that we acquire and maintain. We are committed to the highest standards of information security. To that end, our internal controls and safeguards are regularly revised and updated. Our security policy is based upon the ISO standard which calls for a framework for managing information security including Organization Security (e.g., document controls), Personnel Security, Physical and Environmental Security, Access Control and Compliance. By virtue of this approach, we also comply with various statutes that impose security standards such as Gramm-Leach-Bliley. Our company-wide security spending is 12 percent of total technology spending, which is within the "Gartner benchmark" of 10-14 percent.

With respect to the accuracy of data, our Company believes that everyone should have a right of access to information about them, irrespective of the type, source or use of the information. Using the principles of the Fair Credit Reporting Act as a model, this

would include providing consumers with the right to access their information, the right to question the accuracy and prompt a review, and the right to comment if a negative record is found to be accurate.

The following provides a list of the companies that ChoicePoint has acquired since 2000.

2000:
DBT Online (merger)
Statewide Data Services
Practical Computer Concepts, Inc.
Fraud Defense Network
RRS Police Records Management, Inc.
VIS'N Service Corporation
National Safety Alliance

2001:
Pinkerton's Inc.
Marketing Information & Technology Inc. (MITI)
Insurity Solutions, Inc.
The Bode Technology Group, Inc.
Bti Employee Screening Services, Inc.
ABI Consulting, Inc.
National Medical Review Offices, Inc. (certain assets)

2002:
L&S Report Service, Inc.
Accident Report Services, Inc.
Resident Data, Inc.
Vital Check Network, Inc.
Experian Information Solutions, Inc. (certain parts)
Total eData Corporation

2003:
CITI NETWORK, Inc.
Bridger Systems, Inc.
insuranceDecisions, Inc.
TML Information Services, Inc.
Identico Systems, LLC
Mortgage Asset Research Institute, Inc.
The List Source, Inc.
National Data Retrieval, Inc.

2004:
USA Hire, LLC
Priority Data Systems, Inc.
InsurQuote, Inc.
AIG Technologies, Inc.
Investigations Technologies, LLC
Service Abstract Corp.
ADREM Profiles, Inc.
Charles Jones, LLC and Superior Information Services, LLC
The Templar Corporation
iMapData.com, Inc. - (Jan. 2005)

2005:
i2 Limited (UK)
Magnify
EzGov

The Honorable Gene Green

1. Do you agree that consumers should be notified when their information is sold to a company or third party for commercial use?

   No. Much of the information we provide is compiled from publicly available sources such as Secretary of State offices, departments of motor vehicles, and directory products that are already in the public domain. Moreover, to the extent that information is not compiled from public record sources, several statutes and regulations (e.g., FCRA, Gramm-Leach-Bliley) already protect consumers by restricting how such data may be used. Finally, requiring such notification would hinder many transactions that benefit consumers (e.g., obtaining insurance or renting an apartment) and businesses (e.g., pre-employment screening).

2. Exactly what information is contained in a "National Comprehensive Report" compiled by ChoicePoint?

   See attached sample report.

3. What is the process for ordering a "National Comprehensive Report" from ChoicePoint?

   Credentialed customers may order a report through our website: www.choicepointonline.com or through a toll-free telephone number.

4. How much does ChoicePoint charge for a "National Comprehensive Report"?

   See response to Question 5.

5. What does ChoicePoint charge for creating a report containing information not covered by the Fair Credit Reporting Act?

   ChoicePoint performs a lot of non-FCRA services in many business units other than Public Record Group. That said, different reports have different prices-

   - ***Retail rates range from $3 to $17 for Public Record searches and reports provided through our online interface.***
   - ***High volume, system-to-system users could pay as low as $.25 for some searches.***
   - ***Customized, non-FCRA research performed by our Business Information Services unit could cost hundreds of dollars.***

6. A March 8, 2005 MSNBC article, "ChoicePoint Files Found Riddled with Errors" states that a person's report from ChoicePoint revealed "possible Texas criminal history". Do you believe it is fair to consumers to report the possibility of criminal activity without confirming whether the person has been charged for committing a crime?

   See response to Dingell Question 3.

7. Does ChoicePoint check the validity of the data you sell to other companies and law enforcement? If so, what are the processes and procedures used to do so?

As a data aggregator, we do not feel qualified to judge the accuracy of data (i.e., we don't know if a tax lien is accurate or not). As noted above, we provide a full disclaimer to our customers with respect to the accuracy and completeness of data contained in our reports.

The Honorable Marsha Blackburn

1. When you discover that you have sold information to a person or organization that is going to use it for identity theft, what actions do you take? What do you do with the money – do you give it to the consumers, deposit it in the bank, or use it to prosecute the identity thieves?

   In circumstances where we believe someone is accessing or attempting to access information for inappropriate purposes, ChoicePoint will work with law enforcement officials to investigate fully the facts of the potential breach. In the event a breach has occurred, we work with law enforcement to pursue full prosecution of the criminals perpetrating the crime.

2. Do you perform any preliminary investigation of a company that you sell info to? What standards do you have in place to make sure that the client is not an identity theft ring?

   ChoicePoint's customer credentialing process has been strengthened in recent months. We are requiring additional due diligence such as bank references and site visits before allowing businesses access to personally identifiable information. We are also re-credentialing broad sections of our customer base, including our small business customers.

   We have decided to centralized the credentialing processes for all business units that have products and services that include personally identifiable information. In addition, ChoicePoint has created an independent office of Credentialing, Compliance and Privacy that will ultimately report to our Board of Directors' Privacy Committee. This office will oversee improvements in the customer credentialing process, the expansion of a site-visit based verification program, and implementation procedures to expedite the reporting of incidents. This office will also be responsible for the Company's compliance with local, state and federal privacy laws, regulations and Company policies.

3. Do you perform regular audits of procedures and internal controls to safeguard information before you sell it to your clients? What audits do you do to make sure the information you have gathered is accurate?

   We understand the importance of protecting the data that we acquire and maintain. ChoicePoint is committed to the highest standards of information security.

   Security is an important organization within ChoicePoint. Our security policy is based upon the ISO standard which calls for a framework for managing information security including organization security (e.g., document controls), personnel security, physical and environmental security, access control and compliance. By virtue of this approach we also comply with various statutes that impose security standards such as Gramm-Leach-Bliley.

Our company-wide security spending is 12% of total technology spending, which is within the Gartner benchmark of 10-14%. We utilize internal and external audits of our systems to monitor their security.

4. How many transactions of sale of consumer information occur each day? What is your yearly gross revenue from sales of consumer information?

   Our platforms contain information on both businesses and individuals. We do not track revenue based on whether a search focuses on an individual or a business. In the past year, slightly over 20 million customer-initiated searches were made against our databases. Many searches (like a phone number search) cannot be definitively determined to be consumer or business related. We estimate that between 75% and 80% of searches request data regarding an individual. This includes government and private sector searches

5. What is the average revenue per consumer in a sale?

   Different reports have different prices-

   - ***Retail rates range from $3 to $17 for Public Record searches and reports provided through our online interface.***
   - ***High volume, system-to-system users could pay as low as $.25 for some searches.***
   - ***Customized, non-FCRA research performed by our Business Information Services unit could cost hundreds of dollars.***

6. Have you sold information on American consumers to foreign companies or to foreign governments? Please give this committee a complete account of these foreign transactions – to whom, # consumers, price negotiated, and time of sale.

   ChoicePoint has a very limited number (less than 125) of active accounts located outside the United States.

   Access to Personally Identifiable Information (PII) on US citizens within these accounts is limited to US Government agencies, a few foreign law enforcement agencies (primarily Canadian, Bahamian and Bermudan) working in cooperation with US law enforcement, and foreign offices of US registered multinationals.

   As part of recently announced product changes, we will deliver identity verification and fraud services to foreign offices of US companies, traditional services to US law enforcement agencies and government agencies in foreign countries and will support foreign law enforcement agencies in cooperation with US law enforcement agencies.

National Comprehensive Report Plus Associates

03/07/2005 - 10:30 AM - Reference: Nat-Comp-Assoc

NOTE: This is a sample report. Any reference to actual persons, places, or events is purely coincidental.

Lightly shaded boxes (like this one) appear throughout this sample report and explain the content of various sections. These explanations do not appear in actual reports.

NOTE: The data returned in actual reports *may* or *may not* be displayed as shown below. Please contact a ChoicePoint Sales or Customer Support representative at 1-800-279-7710 for more details about the information available to your specific industry.

NOTE: Clicking underlined hyperlinks within a report will take you to either a detail for the specific record, or to a related search screen (per the current report).

Understanding Report Icons – The following icons may appear in various places throughout a report:

	Related Search Icon – Clicking this icon opens a Related Search window in which you may view a list of databases that contain related searches (as well as those where no information was found). This new window also allows you to run a search from within the current report. Depending on the report section that you are in, some Related Search icons will present you with a choice of criteria to be used in conducting the search. **Example:** Clicking this icon next to a Social Security Number opens a "Related Searches Based On SSN (xxx-xx-xxxx)" window. A list of databases containing that SSN is displayed along with the number of matches in each. Simply select the database of your choice to run an additional search on that SSN.
	Report Icon – Clicking this icon allows you to order a report from within the current report. **Example:** Clicking this icon next to a person's name will open the Individual Report Order Form with their name and address fields pre-populated.
	Telephone Icon – Clicking this icon next to a telephone number will open a Real Time Phone Directories search – providing up-to-the-minute telephone information - with name and address fields pre-populated.
	Dollar Sign Icon – Clicking a hyperlink with this icon next to it will cost the user an additional fee. Hovering a mouse over the icon will display the fee that will be incurred.

ZACHARY K THUL

SSN: 960-45-XXXX issued in New York between 1968 and 1970

** ALERT ** A Death Claim was filed for SSN 960-45-XXXX in JAN 2055.

Death Date: 01/13/2055

Death Last Name: THUL

Death First Name: ZACHARY

DOB: 01/XX/1955

User Supplied Information

User Supplied Information shows the criteria used to generate the report.

Last Name:	THUL
First Name:	ZACHARY
Middle Initial:	K
SSN:	960-45-XXXX
DOB:	01/XX/1955
Address 1:	7891 W FLAGLER ST MIAMI, FL 33180
Address 2:	305 WAYBREEZE BLVD COLUMBUS, OH 34209
Address 3:	4833 STORM ST APT I-33 SPRINGFIELD, OH 34443

ns Available In Report

Click on links to see detail

The 'Sections Available in the Report ' portion only appears when viewing the report in a web browser. Clicking a link provides the ability to view a particular section without having to scroll through the entire report. Each section's heading contains a link to return you to the Top of the report.

Possible AKAs for Subject	3 Records
Possible Other Social Security Numbers Associated with Subject	2 Records
Possible Other Records and Names Associated with Social Security Numbers	2 Records
Possible Driver Licenses	2 Records
Possible Addresses Associated with Subject	5 Records
Possible High Risk Address	2 Records
Possible Infractions	1 Record
Phone Listings for Subject's Addresses	2 Records
Possible Florida Sexual Predator	1 Record
Possible Florida Felony/Probation/Parole	2 Records
Possible Real Property Ownership and Deed Transfers	2 Records
Possible Property Owners of Subject's Addresses	1 Record
Possible Deed Transfers	1 Record
Possible Vehicles Registered at Subject's Addresses	2 Records
Possible Real-Time Vehicle Registrations	1 Record
Possible Criminal Offenders	1 Record
Possible Watercraft	1 Record
Possible FAA Aircraft Registrations	1 Record
Possible UCC Filings	2 Records
Possible Bankruptcies, Liens and Judgments	1 Record
Possible Professional Licenses	1 Record
Possible FAA Pilot Licenses	1 Record
Possible DEA Controlled Substance Licenses	1 Record
Possible Hunting and Fishing Licenses	2 Records
Possible Business Affiliations (includes Officer Name Match)	1 Record
Possible Fictitious Business Names (DBA)	1 Record
Possible Relatives	2 Records
Other People Who Have Used the Same Address of the Subject	2 Records
Possible Licensed Drivers at Subject's Addresses	4 Records
Neighbor Listings for Subject's Addresses	18 Records

Possible AKAs for Subject

(3 Records) Top

Name	SSN	Date of Birth
THUL, ZACK	960-45-XXXX	01/XX/1955
THUL, ZACK K	960-45-XXXX	01/XX/1955
THUL, ZACK	690-45-XXXX	02/XX/1955

** ALERT ** A Death Claim was filed for SSN 690-45-XXXX in FEB 1993.

Possible Other Social Security Numbers Associated with Subject

(2 Records) Top

Subjects will frequently be linked to other names. The most common reasons for this are: 1) Typographical errors, 2) Jointly filed public records which list both the subject and the second name, 3) Father and son who have the same name, and 4) Fraudulent use of a Social Security number. Related Search icons are present only in reports displaying full Social Security Numbers.

Name	SSN	Date of Birth
THUL, ZACHARY K	690-45-XXXX	01/XX/1955
THUL, ZACHARY K	660-45-XXXX	04/XX/1938

** ALERT ** A Death Claim was filed for SSN 660-45-XXXX in FEB 1993.

Possible Other Records and Names Associated with Social Security Numbers (2 Records) Top

Related Search icons are present only in reports displaying full Social Security Numbers.

Name	SSN	Date of Birth
KIRBY, LOARDA J JR	960-45-XXXX	01/XX/1960
KIRBY, LORADA J JR	960-45-XXXX	01/XX/1960

Possible Driver Licenses (2 Records) Top

Driver License information is included in a report if both the name (first and last) and the date of birth match the subject's information. Common names may generate multiple matches that may or may not be related to the subject.

7891 W FLAGLER ST MIAMI, FL 33180

Name:	THUL, ZACHARY KENNETH	**DOB:**	01/XX/1955
DL#:	T432117550XXX	**Issue State:**	FL
Issue Date:	12/13/1999	**Expire Date:**	01/XX/2006
Height:	5' 08"	**Weight:**	165
Eye Color:	BLUE	**Hair Color:**	BROWN
Previous DL State:	OH	**Previous DL#**	275748XXX
SSN:	592-03-XXXX		

4833 STORM ST APT I-33 SPRINGFIELD, OH 34443

Name:	THUL, ZACHARY K	**DOB:**	01/XX/1955
DL#:	275748XXX	**Issue State:**	OH
Issue Date:	12/28/1994	**Expire Date:**	01/XX/2001
Height:	5' 08"	**Weight:**	150
Eye Color:	BLUE	**Hair Color:**	BROWN
Previous DL State:	NY	**Previous DL#**	T12345678XXX
SSN:	960-45-XXXX		

Possible Addresses Associated with Subject (5 Records) Top

The addresses and phone numbers listed here are reported by consumer reporting agencies, proprietary sources, and public records. Unlisted mobile, cell, or other "hard to locate" phone numbers may also be listed *if reported by the subject*. Dates in the Date Range column represent the *first and last reported* dates linking the subject to the address.
NOTE: Addresses without date ranges will appear at the bottom of the address list. Such addresses may be current or historical. Addresses accompanied by the Telephone icon are not confirmed.

Date Range	Address	Source
09/1997 - 10/2003	** 7891 W FLAGLER ST MIAMI, FL 33180 (305) 555-1234 *** 786	Consumer Bureau 1 Consumer Bureau 2 Consumer Bureau 3
06/1994 - 08/1997	* 4833 STORM ST APT I-33 SPRINGFIELD, OH 34443 (555) 555-1935	Consumer Bureau 1 Consumer Bureau 2
07/1994 - 07/1994	4833 STORM ST I33 ☎ SPRINGFIELD, OH 34443	Consumer Bureau 1 Composite Info

	(555) 555-1935	
12/1992 - 04/1995	305 WAYBREEZE BLVD ☎ COLUMBUS, OH 34209 (555) 123-4567	Consumer Bureau 2
	70 REARVIEW DR ☎ RIVERBEND, NY 11903	Consumer Bureau 2 Consumer Bureau 3

* Address verified by current phone listing.
** Address and phone number verified by current phone listing.
*** Other Possible Area Code(s)

Possible High Risk Address

(2 Records)

A High Risk Address is a business address with a higher propensity for fraud as identified through anti-fraud units of state, municipal and federal law enforcement agencies along with actual addresses where fraud has been established. A High Risk Address is based on the Census Bureau's 6-digit Standard Industrial Code (SIC Code). The U.S. Government classifies all businesses with specific SIC codes that help identify industry and product types.

High Risk Addresses include (but are not limited to) addresses of licensed gun dealers, known mail-drop locations, those with a history of known insurance fraud, or businesses of medical providers with a history of known Medicare fraud. The ten most current addresses associated with the subject of the report are run through the High Risk Address database to identify any hits. If a match is found, an alert message is displayed along with the matched address(es), phone number(s) and Risk Indicator/Classification.

Alert - The Following High Risk Address(es) Matched Your Subject's Address History

7891 W FLAGLER ST MIAMI, FL **(305) 555-1234**

Risk Description:	Firearms License	**License:**	98803107C600397
Risk Description:	Firearms License	**License:**	98803107A700488
Risk Description:	Firearms License	**License:**	98803108A700489
Risk Description:	Firearms License	**License:**	98803107C735457

305 WAYBREEZE BLVD COLUMBUS, OH **(555) 123-4567**

Risk Description:	SIC Code	**SIC Code:**	801101	**SIC Description:**	PHYS & SURGEONS
Risk Description:	SIC Code	**SIC Code:**	801104	**SIC Description:**	CLINICS
Risk Description:	SIC Code	**SIC Code:**	804922	**SIC Description:**	PSYCHOLOGISTS
Risk Description:	SIC Code	**SIC Code:**	839901	**SIC Description:**	DRUG INFO/TREATMENT

Possible Infractions

(1 Record) Top

THIS INFORMATION IS NOT TO BE USED FOR PREEMPLOYMENT PURPOSES.
This data indicates a possible infraction on the searched name; however, this information should be verified through the agency that reported the infraction.

Infractions information can help to verify possible high-risk identity data in compliance with the USA Patriot Act. This could include a person on the OFAC (Office of Foreign Assets Control) who may have been identified as a possible terrorist or money launderer, or who has been debarred or sanctioned by the US Government.

Record Source	US Dept of Commerce, Bureau of Export Admin, Denied Persons Info
Name	THUL, ZACHARY K
Alias Name	SMITH, JOHN R
Alias Name	DOUGH, JOHN R
Address	7891 W FLAGLER STREET
City	MIAMI
State	FL
Zip	33180
Country	U.S.A.
Date of Birth	01/XX/1955

Other information DOB 01/XX/1955, SSN 960-45-XXX, PASSPORT NO. 123456789 <U.S.A.>.

Phone Listings for Subject's Addresses (2 Records) Top

By comparing the list of *Possible Addresses Associated With Subject* with the listed phone numbers in one of the Phones databases, the report finds phone numbers reported at the given address. The result in the first listing below may indicate that a multi-unit building is located at the address.

7891 W FLAGLER ST, MIAMI, FL 33180

Over 100 phone numbers found, only same last name considered.
** No Phone numbers found during search **

4833 STORM ST SPRINGFIELD, OH 34443

Name: ACME RENTALS **Phone:** (555) 555-1935

305 WAYBREEZE BLVD COLUMBUS, OH 34209

Name: THUL ZACHARY **Phone:** (555) 498-5525

Possible Florida Sexual Predator (1 Record) Top

The Florida Sexual Predators database contains information on Sexual Predators *and* Offenders. A ***sexual predator*** is someone who has been convicted or is found guilty (after 10/01/93) of any capital, life, or first degree felony violation of Chapter 794 which includes: sexual battery by persons 18 years or older upon victims less than 12 years of age. A ***sexual offender*** is any person convicted of committing, attempting, conspiring, or soliciting to commit any of the following: luring or enticing a child under the age of 12 into a structure, dwelling, or conveyance for other than a lawful purpose.

Name: ZACHARY K THUL
Type: SEXUAL OFFENDER
Address: 7891 W FLAGLER ST
MIAMI, FL 33180
County: MIAMI-DADE
Address Type: RESI
Address as of Date: 12/06/2003
Doc Number: L21234
Offense: LEWD, LASCIVIOUS CHILD
Status: RELEASED

Possible Florida Felony/Probation/Parole (2 Records) Top

Florida Felony/Probation and Parole information is derived from the Florida Department of Corrections and is accessed through the Florida Convictions database or the Criminal Offenders database.

ZACHARY K THUL

DOB: 01/XX/1955 **SSN:** 960-45-XXXX **Sex:** Male **Race:** White
Status: Active Inmate
DOC Number: W62236

Case Number: 9729447
Commitment: Prison Inmate **County Convicted:** BROWARD
Offense Date: 12/01/1997 **Sentence Date:** 06/15/2000
Maximum Term: 3 Years 1 Month 24 D
Offense: NCIC Code 1317 AGG ASSLT-W/WPN NO INTENT TO KILL

Case Number: 9729447

Commitment:	Prison Inmate	**County Convicted:**	BROWARD
Offense Date:	12/04/1997	**Sentence Date:**	06/15/2000
Maximum Term:	3 Years 1 Month 24 D		
Offense:	NCIC Code 9512 COCAINE-SALE/MANUF/DELIV.		

Notice This database is supplied by the State of Florida, Department of Corrections. As such Choicepoint Inc. does not warrant the accuracy or comprehensiveness of these records.

Possible Real Property Ownership and Deed Transfers (2 Records) Top

In this instance, two property records were found in Real Property that matched the subject's Last Name, First Name, and Address. The most current tax roll record is displayed first, and is followed by a deed history. Selecting the hyperlinked Parcel Number will take you to a detail screen for the record or open a Related Search window. If no tax roll information is found, deed information may instead appear in the following *Possible Deed Transfers* section. **NOTE:** The message following the second property indicates that additional records in Real Property match the subject's *name*, but that none of those records had a situs address that matched an address found at the top of the report.

4833 STORM ST SPRINGFIELD, OH 34443

Owner Name:	THUL, ZACHARY		
Assess State:	Ohio	**County:**	CLARK
Parcel Number:	998-8748-9448	**Type:**	SINGLE FAMILY
Short Legal Description:	LT 12 BLK B PB C/79		
Document Number:	98765432	**Recorded Date:**	05/27/1994
Situs Address:	4833 STORM ST I-33 SPRINGFIELD, OH 34443-4321	**Book:**	7613
Mailing Address:	7891 W FLAGLER ST MIAMI, FL 33180-6789	**Page:**	1689
Assessment Year:	1995	**Tax Year:**	1995
Assessed Land Value:	$24,000	**Market Land Value:**	$26,000
Assessed Improvements:	$26,000	**Market Improvements**	$3,000
Total Assessed Value:	$29,000	**Total Market Value:**	$55,000
Most Recent Sale:	$45,000	**Prior Sale Price:**	$32,000

Ohio Deed Transfer Records - County of: CLARK

Parcel Number:	T545663
Legal Description:	LT 12 BLK B PB C/79
Sale Price:	$84,000
Loan Amount:	$67,000
Contract Date:	08/14/1995
Deed Type:	Mortgage Deed
Ownership Right:	Married Man
Relationship Type:	Single Man
Resale/New Construction:	Resale
Foreclosure	No
Refinance:	Yes
Lender:	TIDEWATER BANK
Title Co:	AMERICAN TITLE COMPANY
Situs Address:	305 WAYBREEZE BLVD COLUMBUS, OH 34209

Seller(s):	ZACHARY K THUL CLAIRE M THUL
Seller Address:	305 WAYBREEZE BLVD COLUMBUS, OH 34209
Buyer(s):	SMITH BART O & BRENDA K
Buyer Address:	503 BREEZEWAY BLVD COLUMBUS, OH 34210

70 REARVIEW DR, RIVERBEND NY 11903

Owner Name:	THUL, ZACHARY		
Assess State:	New York	**County:**	WESTCHESTER
Parcel Number:	987-6543-2109	**Type:**	SFR
Short Legal Description:	'02 SPLIT LOT 1 PER ZBA		
Document Number:	87654321	**Recorded Date:**	03/18/1989
Situs Address:	70 REARVIEW DR RIVERBEND, NY 11903-4567	**Book:**	006455
Mailing Address:	70 REARVIEW DR RIVERBEND, NY 11903-4567	**Page:**	000725
Assessment Year:	2002	**Tax Year:**	2002
Assessed Land Value:	*$2,000	**Market Land Value:**	$100,000
Assessed Improvements:	*$3,000	**Market Improvements**	$8,000
Total Assessed Value:	*$6,000	**Total Market Value:**	$108,000
Most Recent Sale:	$80,000	**Prior Sale Price:**	$72,000

* New York assessed values are a percentage of the actual amount

A manual search of Real Property using the name THUL ZACHARY K is recommended. 11 additional property records exist (including historicals) but are not included, as they do not match all necessary criteria.

Possible Property Owners of Subject's Addresses (1 Record) Top

Information in this section is returned based upon a match of the subject's full address. Only the most recent tax roll information is displayed. Hyperlinked Parcel Numbers will take you to detail screens or Related Search windows for those records. Any deeds for these addresses that cannot also be linked to a tax roll record will not display in Possible Deeds Transfers section that follows.
This section is often helpful in providing landlord information.

4833 STORM ST SPRINGFIELD, OH 34443

Owner Name:	THUL, ZACHARY K		
Assess State:	Ohio	**County:**	CLARK
Parcel Number:	998-8748-9448	**Type:**	SINGLE FAMILY
Short Legal Description:	LT 12 BLK B PB C/79		
Document Number:	98765432	**Recorded Date:**	05/27/1994
Situs Address:	4833 STORM ST I-33 SPRINGFIELD, OH 34443-4321	**Book:**	7613
Mailing Address:	7891 W FLAGLER ST MIAMI, FL 33180-6789	**Page:**	1689
Assessment Year:	1995	**Tax Year:**	1995
Assessed Land Value:	$24,000	**Market Land Value:**	$26,000
Assessed Improvements:	$26,000	**Market Improvements**	$3,000
Total Assessed Value:	$29,000	**Total Market Value:**	$55,000
Most Recent Sale:	$45,000	**Prior Sale Price:**	$32,000

Ohio Deed Transfer Records - County of: FRANKLIN

Parcel Number:	998-8748-9448
Legal Desc:	LT 12 BLK B PB C/79
Sale Price:	$84,000
Loan Amount:	$67,000
Contract Date:	08/14/1995
Deed Type:	Mortgage Deed
Ownership Right:	Married Man
Relationship Type:	Single Man
Resale/New Construction:	Resale
Foreclosure:	No
Refinance:	Yes
Lender:	LIBERTY SAV BK
Title Co:	GULFSTREAM TITLE COMPANY INC
Situs Address:	305 WAYBREEZE BLVD COLUMBUS, OH 34209
Seller(s):	ZACHARY K THUL CLAIRE M THUL
Seller Address:	305 WAYBREEZE BLVD COLUMBUS, OH 34209
Buyer(s):	SMITH BART O & BRENDA K
Buyer Address:	503 BREEZEWAY BLVD COLUMBUS, OH 34210

Possible Deed Transfers (1 Record) Top

The *Possible Deed Transfers* Section includes records that returned no corresponding tax roll information and therefore contains *only* deed information.

Florida Deed Transfer Records - County of: MIAMI-DADE

Parcel Number:	94-21-49-37-0690
Legal Desc:	FLAGAMI 3RD ADDN PB 17-120B LOT 16 BLK 212
Sale Price:	$89,000
Loan Amount:	$69,000
Contract Date:	08/11/2001
Lender:	TIDEWATER BANK
Title Co:	AMERICAN TITLE COMPANY
Situs Address:	7891 W FLAGLER ST MIAMI, FL 33180
Seller(s):	ZACHARY K THUL CLAIRE M THUL
Seller Address:	7891 W FLAGLER ST MIAMI, FL 33180
Buyer(s):	DOUGH JOHN R & JANE B
Buyer Address:	4791 W 8TH AVE HIALEAH, FL 33012

Possible Vehicles Registered at Subject's Addresses (2 Records) Top

AutoTrackXP reports locate vehicles by the subject's addresses – regardless of the name on the vehicle registration. If there are over 10 vehicles at a particular address, we will only match vehicles at that address that also match the last name of the subject. *It is possible to find leased vehicles.* A Report icon will appear next to the owner's name in cases where the owner is *not* the subject of the report.
NOTE: When ordering the National Comprehensive and National Comprehensive Plus Associates report, step three of the Report Order Form allows you to limit vehicle information returned "To Those Having a Registration Date Within the Last 2 Years," and/or "To Those Associated With the Report Subject."

70 REARVIEW DR, RIVERBEND NY 11903

Plate:	K387KJ		
Lien Holder:	AMSOUTH BANK		
Address:	P O BOX 1234 NEW YORK, NY 11945		
Owner:	CLAIRE M THUL		
State:	NY		
Date Registered:	08/14/1996	**Expire Date:**	08/30/1998
Title:	76174123	**Title Date:**	08/14/1996
VIN:	2B5CD3595EK253648		
Color:	BLUE		
Year:	1999		
Description:	DODGE CARAVAN DODGE CARAVAN - 3.0L V6 SMPI OHV 12V MINIVAN		

7891 W FLAGLER ST, MIAMI, FL 33180

Plate:	ID036H		
Owner:	ZACHARY K THUL		
State:	FL		
Date Registered:	04/28/1999	**Expire Date:**	10/30/1999
Title:	77465432	**Title Date:**	09/29/1998
VIN:	1GCCS144X8144822		
Color:	UNKNOWN COLOR - UNK		
Year:	1997		
Description:	CHEVROLET S10 PICKUP CHEVROLET S10 PICKUP - 2.2L L4 EFI OHV 8V PICKUP		

70 REARVIEW DR, RIVERBEND NY 11903

**26 Vehicles found, only same last name(s) are listed **

Due to privacy regulations instituted by individual states, Vehicle data from all states may not be available.

Possible Real Time Vehicle Registrations (1 Record) Top

A maximum of 25 records can be returned in this section based on the subject's last name and most current address. If no data is returned for the most current address, the address will still be listed, but with the message "Data for the subject was not found" displayed below it. In this event, data linked to the *second* most current address will be displayed. This section will not appear in reports if no data is returned for either address.

Notice Vehicles Registered to Last Name and Subject's Current Address

7891 W FLAGLER ST, MIAMI, FL 33180

VIN SERVICES REPORT FOR USE BY LEGITIMATE BUSINESS FOR INFORMATION VERIFICATION OR CORRECTION

Registered Owner: ZACHARY K THUL $

VIN: YV361112S960KXW72

Make Model: VOLVO S90 **Model Year:** 2005

Possible Criminal Offenders

(1 Record) Top

THIS INFORMATION IS NOT TO BE USED FOR PRE-EMPLOYMENT PURPOSES. As this INFORMATION is compiled from individual sources, ChoicePoint Public Records Inc. does not warrant the accuracy or comprehensiveness of these records. This may or may not be a complete criminal history. The data indicates a possible criminal history on the searched subject; however, a full file should be pulled directly from the agency to confirm the proper identity of the subject and any additional information available.

Depending on your level of access to AutoTrackXP, Criminal Offenders information may be pulled into a report from the report request form. The Criminal Offenders database includes information about individuals who are incarcerated due to felony and misdemeanor convictions and includes data (some historical) from 30 states.

Offender Name: THUL, ZACHARY K

DOB: 01/XX/1955 **SSN:** 960-45-XXXX **Sex:** MALE **Race:** WHITE

Status: ACTIVE PROBATION/PAROLE

Source: Ohio Parole

Offense: LEWD, LASCIVIOUS CHILD U/16

Offense Date: 01/31/1983

State Convicted: OH **County Convicted:** MORROW

Case Number: 9876543 **Commitment:** PRISON INMATE

Conviction Date: 03/30/1983 **Sentence Date:** 03/31/1983

Total Sentence: 3 Years **Maximum Sentence:** 20 Years

Probation Sentence: 5 Years

CAUTION: An individual with this name has submitted fingerprints that indicate that he or she is NOT the subject of this record. The Ohio Department of Rehabilitation and Correction has issued a letter to this individual, confirming that he or she is NOT the subject of this record. Fingerprint verification is the only way to confirm that an individual is or is not the subject of a record.

Possible Watercraft

(1 Record) Top

Possible Watercraft information can provide access to state registrations and boating accidents.

Owner: THUL ZACHARY K (Historical)

Co-owner: THUL CLAIRE M

Address: 7891 W FLAGLER ST
MIAMI, FL 33180

Year: 1988 **Length:** 41.9'

Make: DONZI

Registration Number: FL FL9584LC **State Registered:** FL

Registration Date: 12/26/1990

Title Number: 0079687544

Hull ID: DNAM4206I769 **Hull Construction:** FIBERGLASS

Use: PLEASURE

Propulsion: INBOARD/OUTBOARD **Fuel:** GAS

Due to privacy regulations instituted by individual states, Watercraft data from all states may not be available.

Possible FAA Aircraft Registrations

(1 Record) Top

Name: THUL ZACHARY K

Year:	1972
Make:	CESSNA
Model:	172M
N-Number:	N90190
Aircraft:	FIXED WING SINGLE ENGINE
Address:	7891 W FLAGLER ST MIAMI, FL 33180-1234

Possible UCC Filings

(2 Records) Top

UCC stands for Uniform Commercial Code, which governs commercial transactions. UCC Filings in an AutoTrackXP Report can include debtor and secured party information. **TIP** - Click the Date hyperlink to access the original financing statement, file number and date of transactions.

Original File #:	8219252	**Date:**	01/17/2001		
Action:	INITIAL FILING	**Date:**	06/05/1997	**File State:**	FLORIDA
Debtor:	THUL ZACHARY K	**Address:**	7891 W FLAGLER ST MIAMI FL 33180		
Secured Party:	SOUTHEAST FLORIDA FEDERAL BANK	**Address:**	123 ANDREWS AVE PO BOX 123 FORT LAUDERDALE FL 33301		
Collateral:	GENERAL EQUIPMENT				

Original File #:	910007323403	**Date:**	10/31/1991		
Action:	ORIGINAL	**Date:**	10/31/1991	**File State:**	FLORIDA
Action:	TERMINATION	**Date:**	10/17/1994	**File State:**	FLORIDA
Debtor:	JOHNSON AMBULANCE SERVICE	**Address:**	2500 WESTLAKE BLVD MESQUITE TX 75149		
Secured Party:	KEYS COMMUNITY BANK	**Address:**	PO BOX 4321 KEY LARGO FL 33037		

Possible Bankruptcies, Liens and Judgments

(11 Records) Top

Pursuant to amendments to Section 2075 of Title 28, the Federal Rules of Bankruptcy Procedure and Official Forms, effective December 1, 2003, Social Security Numbers in Bankruptcy filings will be truncated so that only the last four digits of the number will be made available. This truncation is handled at the federal court level.

A bankruptcy is a legal proceeding that protects a debtor from legal action by some creditors. In this report, one bankruptcy was found that matched the subject's Social Security number and address.

Court Location:	FLORIDA FED COURT-MIAMI		
Filing Type:	Chapter 7 Discharge	**Filing Date:**	10/29/1997
Filing State:			
Case Number:	9733341	**Release Date:**	02/04/1998
Plaintiff Attorney:			
Judgment Docket Number:		**Judgment Date:**	
Certificate:			
Sch. 341 Date:	12/04/1997		
Unlawful Detainer:			
Creditor/Plaintiff:			
Plaintiff/Firm:	SMITH AND JONES	**Amount:**	$5,500
Debtor:	THUL ZACHARY K, THUL CLAIRE M		
SSN/Tax ID:	960-45-XXXX, 987-65-XXXX		
Address:	7891 W FLAGLER ST		

	MIAMI FL 33180
Liabilities:	$200,000
Assets:	$2,000
Assets Available:	No
Judge Initials:	JEB
Attorney:	SMITH JOHN R
Address:	561 BISCAYNE BLVD #561, MIAMI FL 33123

Possible Professional Licenses (1 Record) Top

The Professional Licenses database can be used to: 1) Narrow down common names (such as John Smith) to only those who are Registered Nurses), 2) Verify license information, 3) Prove that a license is in good standing, and 4) Locate possible employment information. Hyperlinked Names will take you to detail screens or Related Search windows for those records. To view the types of Professional Licenses available, click the *Online Support* button from the Main Menu.

Type:	OHIO		
License Type:	LICENSED INDEPENDENT SOCIAL WORKER		
License Number:	42389	**Status:**	ACTIVE
Issue Date:	01/15/2000	**Expire Date:**	01/31/2005
Original Date:	01/10/1990	**Renew Date:**	01/10/2005
SSN:	960-45-XXXX	**DOB:**	01/XX/1955
Phone:	(555) 555-1935		
Full Name:	THUL, ZACHARY K		
Address:	4833 STORM ST I-33 SPRINGFIELD, OH 34090		
County:	CLARK		

Possible FAA Pilot Licenses (1 Record) Top

Name:	THUL, ZACHARY K
FAA Class:	PRIVATE PILOT
FAA Rating:	SINGLE ENGINE LAND
Medical Class:	THIRD CLASS-VALID FOR 24 MONTHS
Medical Date:	07/19/1998
FAA Region:	NORTHWEST/MOUNTAIN - CO, ID, MT, OR, UT, WA, WY
Address:	4833 STORM ST I-33 SPRINGFIELD, OH 34090

Possible DEA Controlled Substance Licenses (1 Record) Top

Certain individuals and businesses are required to be registered under the Controlled Substance Act. Physicians, dentists, and veterinarians are among this group.

Business:	PRACTITIONER (Historical)
Name:	THUL, ZACHARY K MD
Expire Date:	09/30/1999
Address:	7891 W FLAGLER ST MIAMI, FL 33180
Drug Schedule:	II, IIN, III, IIIN, IV, V

Possible Hunting and Fishing Licenses (2 Records) Top

This section contains information on hunting and fishing licenses information. Data in this section includes information from 22 states. It is possible for the Source State to be different than the subject's property address if the subject obtained a license in a state other

than the one they reside in. "Not Provided" means that the vendor did not provide the information to ChoicePoint.

Name:	THUL ZACHARY K
Address:	7891 W FLAGLER ST MIAMI, FL 33180
DOB:	01/XX/1955
Source State	FL
Permit Number:	H12345678
License Date:	10/13/2001
Hunting License:	Yes
Fishing License:	NOT PROVIDED
Lifetime Permit:	NOT PROVIDED
License Type:	SPORTSMANS

Name:	THUL ZACHARY K
Address:	7891 W FLAGLER ST MIAMI, FL 33180
DOB:	01/XX/1955
Source State	FL
Permit Number:	F12345678
License Date:	11/18/2000
Hunting License:	NOT PROVIDED
Fishing License:	YES
Lifetime Permit:	YES
License Type:	SALTWATER FISH/SNOOK

Possible Business Affiliations (includes Officer Name Match)

(1 Record) Top

If there are over seven name matches in Corporations, the report will not display any business affiliations (as displayed in the Officer Name Match Only portion).

The current status of this NEW JERSEY Corporation is unconfirmed. Further investigation is required for changes that may have occurred to date.

STETSON HAULING, INC.

Corp State:	FL	**Corp Number:**	1234567	**Status:**	ACTIVE
Affiliation:	CHAIRMAN	**ABI Number:**	7589922662	**ABI Phone:**	(758) 992-2662

Officer Name Match Only (NOT necessarily affiliated)

Matching Name: THUL ZACHARY

OLSON FAMILY PROPERTIES, INC.

Corp State:	NJ	**Corp Number:**	20021234567	**Status:**	ACTIVE
Affiliation:	NAME (REGISTERED AGENT)				

Possible Fictitious Business Names (DBA)

(1 Record) Top

The *Fictitious Business Names (DBA)* section can be helpful in finding information regarding small business assets that might otherwise remain hidden, Determining the true ownership of a company, and Connecting individuals known to be involved in fraudulent activities to small businesses that they have used to hide assets. In addition to providing summary information on the possible DBA(s) a subject may hold, clicking the hyperlinked Business Name gives users access to a Details Page for the business and the means to order a Business Report directly.

The following data is for information purposes only and is not an official record. Certified copies may be obtained from the individual state's department of state.

Business Name:	STETSON HAULING		
Address:	7891 W FLAGLER ST MIAMI FL 33180		
File Number:	G02550589200	**Filing State:**	FL
File Date:	02/26/2002	**Expiration Date:**	12/31/2007
Business Status:	ACTIVE	**Status Date:**	02/28/2002
Owner Name:	THUL ZACHARY		
Address:	7891 W FLAGLER ST MIAMI FL 33180		

Possible Relatives (2 Records) Top

A "Relative" is anyone with the same last name or AKA as the subject who has been linked to one or more of the addresses that appear under *Possible Addresses Associated with Subject*. Clicking on the hyperlinked "relative's" name allows you to view detail for that record and run a report if you wish. Clicking on the Report Icon *next to* the "relative's" name will request a report.

NOTE: When ordering the Basic Report Plus Associates and National Comprehensive Plus Associates reports, step three of the Report Order Form provides the option to define the degree of separation of relatives.
First degree includes people associated with the subject. *Example:* Zack Thul's spouse, Claire Thul.
Second degree includes people associated with the first-degree relatives. *Example:* Claire Thul's sister, Martha Grymes.
Third degree includes people associated with the second-degree relatives. *Example:* Martha Gryme's son, Jerome Grymes (Zack's nephew by marriage).

1. THUL, CLAIRE M

DOB: 12/XX/1954 **SSN:** 987-65-XXXX issued in New York in 1973

Possible AKA: THUL, CLEAR **SSN:** 987-65-XXXX **DOB:** 12/XX/1954

Date Range	Address	Phone
Oct 1994 - Jul 2002	* 305 WAYBREEZE BLVD COLUMBUS, OH 34209	(614) 567-8901 **380
Jul 1995 - Jul 1995	15 ROBY AVE HAMPTON BAYS, NY 11238	
Oct 1994 - Oct 1996	355 LAVERNE AVE COLUMBUS, OH 34492	
Dec 1992 - Dec 1996	70 LAKEVIEW DR RIVERHEAD, NY 11901	

2. THUL, TOMMY

DOB: 12/XX/1957 **SSN:** 345-67-XXXX issued in Illinois between 1971 and 1972

Death Date: 01/1982 ** ALERT ** A Death Claim was filed for SSN 345-67-XXXX in JAN 2004.

Date Range	Address	Phone
Dec 1995 - Dec 1996	599J RR 2 RIVERBEND, NY 11093	(555) 555-4321
Apr 1995 - Aug 1995	355 LAVERNE AVE COLUMBUS, OH 34492	

* Match with one of subject's addresses.

Other People Who Have Used the Same Address of the Subject (3 Records) Top

An "Other" is someone who is linked to one or more of the same addresses as the *subject* of the report, but has a different last name. Multiple (*) indicate multiple address matches with the subject. If there are over 20 individuals found at a particular address, no "Others" will be listed for that address.
NOTE: When ordering the Basic Report Plus Associates and National Comprehensive Plus Associates reports, step three of the Report Order Form provides the option to "Apply Concurrent Others to This Report". Concurrent Others includes information on individuals linked to one or more of the same addresses as the report subject. The ***"Same Time Frame"*** option includes people who have lived at the same address as the subject during the same time. The ***"± 2 Years"*** option includes people who have lived at the same address as the subject during the same time, plus or minus two years from the date range displayed. *Example: if Zack Thul were linked to the address of 7891 West Flagler from 09/1997-10/2001, others would be brought into the report that were linked to that address between the years of 09/1995-10/2003.*

305 WAYBREEZE BLVD COLUMBUS, OH 34209

1. SMITH, MARIE G

DOB: 03/XX/1936 **SSN:** 991-25-XXXX issued in New Jersey in 1962

Date Range	Address	Phone
09/1993 - 09/1994	* 305 WAYBREEZE BLVD COLUMBUS, OH 34209	(555) 123-4567
09/1995 - 09/1996	301 BAYSIDE TER CHARLOTTE, OH 34258	
09/1993 - 09/1994	* 70 REARVIEW DR RIVERBEND, NY 11903	
06/1993 - 06/1993	1505 E I HWY 118 GARLAND, TX 75043	
05/1993 - 05/1993	RR 2 BOX 465F DE QUEEN, AR 71832	
07/1992 - 07/1992	1505 E INTERSTATE 30 GARLAND, TX 75043	
NA - NA	2005 PINEHURST LN 3201 MESQUITE, TX 75150	

2. GARFIELD, TERRY L

DOB: 04/XX/1960 **SSN:** 876-54-XXXX issued in Florida between 1976 and 1977

** ALERT ** SSN 876-54-XXXX was issued to PICKET, T, and a Death Claim for this SSN was filed in JUL 2004.

Date Range	Address	Phone
03/1992 - 07/2001	* 305 WAYBREEZE BLVD COLUMBUS, OH 34209	(987) 543-2109
09/1992 - 03/1994	2345 PUTNAM AVE JACKSONVILLE, FL 32207	
NA - NA	56789 ATLANTIC BLVD JACKSONVILLE, FL 32227	
NA - NA	7654 HABERSHAM CIR JACKSONVILLE, FL 32216	

4833 STORM ST APT I-33 SPRINGFIELD, OH 34443
** No Individuals Found At This Address **

7891 W FLAGLER ST MIAMI, FL 33180
Additional records have been linked to this address. A manual search with this address is suggested, as there are too many records to display in this report.

* Match with one of subject's addresses.

Possible Licensed Drivers At Subject's Addresses (4 Records) Top

The message under the last address below probably indicates that a multi-unit building is located at this address.

4833 STORM ST APT I-33 SPRINGFIELD, OH 34443

Name:	EDWARD H THUL		
DOB:	04/XX/1969	**Height:**	5' 06"
DL#:	T600XXX		
Issue State:	OH	**Issue Date:**	07/27/1994
Expire Date:	04/XX/2000		

70 REARVIEW DR, RIVERBEND NY 11903

** No Drivers Found At This Address**

305 WAYBREEZE BLVD COLUMBUS, OH 34209

Name:	STACY B THUL		
DOB:	05/XX/1962	**Height:**	5' 02"
DL#:	T600XXX		
Issue State:	OH	**Issue Date:**	07/24/1994
Expire Date:	05/XX/2001		

7891 W FLAGLER ST, MIAMI, FL 33180

** 91 Drivers found at this address, only last name considered. **
** No Drivers Found At This Address**

Driver License Information is unavailable for the following states:
ARIZONA, CALIFORNIA, NEW YORK

Neighbor Listings for Subject's Ad s (18 Records)

Neighbor Listings are displayed in an alternating pattern -- back and forth down the street -- starting at the subjects address. Up to 20 neighbors per address may be included.

7891 W FLAGLER ST MIAMI, FL 33180

STATER OFFICE PRODUCTS	7895 W FLAGLER ST	(555) 555-0482
BIG ED'S MUFFLER SHOP	7897 W FLAGLER ST	(555) 555-3358
BUD'S USED CARS	7900 W FLAGLER ST	(555) 555-8288

70 REARVIEW DR, RIVERBEND NY 11903

FELLINGHAM MIKE	73 REARVIEW DR	(555) 555-8697
SCOTT GORDON G	74 REARVIEW DR	(555) 555-6797
GHERSI JOHN	75 REARVIEW DR	(555) 555-6819
ELIAS SIMON	77 REARVIEW DR	(555) 555-2659
SCALCIONE STAN	79 REARVIEW DR	(555) 555-8425
CANGIANO F P	80 REARVIEW DR	(555) 555-5217
CORCORAN STEVE	82 REARVIEW DR	(555) 555-9917

305 WAYBREEZE BLVD COLUMBUS, OH 34209

ALPIN JEFF	304 WAYBREEZE BLVD	(555) 555-2584
AMBROSE A	306 WAYBREEZE BLVD	(555) 555-7553

AHRENDT DAN	307 WAYBREEZE BLVD	(555) 555-1664
APURTON J	309 WAYBREEZE BLVD	(555) 555-0735
ARNOLD ROBY	311 WAYBREEZE BLVD	(555) 555-4071
BAKER C R	314 WAYBREEZE BLVD	(555) 555-7140
BALCHUNAS TERRY	315 WAYBREEZE BLVD	(555) 555-5753
BAMBERGER RICHARD	320 WAYBREEZE BLVD	(555) 555-8203

***** Report section(s) with no matches:**

It is often helpful to know where information about a subject does *not* exist. The list below highlights databases that were accessed while performing your search, but that contained no relevant data to return.

Possible Broward County Felonies and Misdemeanors, Possible Miami-Dade County Warrants, Possible Florida Concealed Weapon Permits, Possible Florida Accidents, Possible Broward County Traffic Citations, Possible Broward County Warrants, Possible Florida Insurance Agents, Possible Florida Tangible Property, Possible Florida Unclaimed Property, Possible Watercraft - USCG Documented Vessels, Possible Florida Boating Citations, Possible Dallas County Criminal Histories, Possible Texas State Criminal History, Possible Marine Radio Licenses, Possible Florida Salt Water Product Licenses, Possible Florida Securities Dealer Registrations, Possible Florida Day Care Licenses, Possible Florida Department of Education, Possible Florida Banking and Finance Licenses, Possible Florida Handicap Parking Permits, Possible Florida Tobacco License, Possible Florida Beverage License, Possible Florida Money Transmitter Licenses, Possible Texas Hunting and Fishing Licenses, Possible Texas Beverage Licenses, Possible U.S. Military Personnel, Possible Oregon Beverage License, Possible Federal Firearms and Explosives License, Possible Significant Shareholders, Possible Trademarks/Service Marks, Possible Texas Trademark Registrations, Possible Florida Fictitious Name, Possible Florida Hotels and Restaurants, Possible Florida Worker's Compensation Claims, Possible Washington Business Registry, Possible Texas Marriages, Probable Carrier Report

Should you have questions or encounter difficulties with your report, the control information below will assist our Customer Support team in providing solutions in a more timely manner. As each report has a unique control number, please have the specific report in question available when contacting us.

*** Option Control Number: NNN1-117-NATCOMPASS ***
*** BOAWPRPT027/02 511164 51116 ***
*** expGate ***

*** * * END OF REPORT * * ***