AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–60

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 13, 2005

Serial No. J–109–11

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

22–293 PDF 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 THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois

DAVID BROG, *Staff Director*
MICHAEL O'NEILL, *Chief Counsel*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin	24
prepared statement	142
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	4
prepared statement	145
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	2
prepared statement	155
Schumer, Charles E., a U.S. Senator from the State of New York	26
prepared statement	181
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	1

WITNESSES

Barrett, Jennifer, Chief Privacy Officer, Acxiom Corporation, Little Rock, Arkansas	33
Curling, Douglas C. President and Chief Operating Officer, ChoicePoint, Alpharetta, Georgia	31
Dempsey, James X., Executive Director, Center for Democracy & Technology, Washington, D.C.	35
Douglas, Robert, Chief Executive Officer, PrivacyToday.Com, Steamboat Springs, Colorado	7
Johnson, Larry, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service, Washington, D.C.	13
Majoras, Deborah Platt, Chairman, Federal Trade Commission, Washington, D.C.	9
Sanford, Kurt P., President and Chief Executive Officer, U.S. Corporate and Federal Markets, LexisNexis, Miamisburg, Ohio	29
Sorrell, William H., Attorney General, State of Vermont, and President, National Association of Attorneys General, Montpelier, Vermont	15
Swecker, Chris, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Washington, D.C.	11

QUESTIONS AND ANSWERS

Responses of Jennifer T. Barrett to questions submitted by Senator Leahy	49
Responses of Douglas Curling to questions submitted by Senators Specter and Leahy	52
Responses of Deborah Platt Majoras to questions submitted by Senators Leahy and Biden	66
Responses of Kurt P. Sanford to questions submitted by Senators Specter and Leahy	79

SUBMISSIONS FOR THE RECORD

Barrett, Jennifer, Chief Privacy Officer, Acxiom Corporation, Little Rock, Arkansas, prepared statement	87
Consumers Union, Gail Hillebrand, San Francisco, California, prepared statement	95
Curling, Douglas C. President and Chief Operating Officer, ChoicePoint, Alpharetta, Georgia, prepared statement	97
Dempsey, James X., Executive Director, Center for Democracy & Technology, Washington, D.C., prepared statement	103
Douglas, Robert, Chief Executive Officer, PrivacyToday.Com, Steamboat Springs, Colorado, prepared statement and attachments	120

Page

Johnson, Larry, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service, Washington, D.C., prepared statement 148
Kuhlmann, Arkadi, Cheif, Executive Officer, ING Direct, Wilmington, Delaware, prepared statement 153
Majoras, Deborah Platt, Chairman, Federal Trade Commission, Washington, D.C., prepared statement 160
Sanford, Kurt P., President and Chief Executive Officer, U.S. Corporate and Federal Markets, LexisNexis, Miamisburg, Ohio, prepared statement 184
Sorrell, William H., Attorney General, State of Vermont, and President, National Association of Attorneys General, Montpelier, Vermont, prepared statement 198
Swecker, Chris, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Washington, D.C., prepared statement 214

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

WEDNESDAY, APRIL 13, 2005

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:30 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Arlen Specter, Chairman of the Committee, presiding.

Present: Senators Specter, Coburn, Leahy, Kohl, Feinstein, Feingold, and Schumer.

OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Chairman SPECTER. It is 9:30 and our practice is to begin these hearings precisely on time. We have a long list of witnesses today, ten in number. We have a vote scheduled for 11:15, and once Senators disperse to go to vote, it is pretty hard to get the attention of the Senators after that. So we are going to be operating under our usual time limit of five minutes for statements by witnesses. All statements will be made a part of the record in full and that will be our method of proceeding.

First, on a brief personal note, I was stopped coming over by a young woman who told me her father has a situation similar to mine. And I get a tremendous number of questions and I am glad to report that I am doing fine with certain treatments. I have a new hair stylist. That is the most marked change in my situation. I have been on the job. We have had the hearings, persevering with the work of the Senate. Some days are better than others, but it is all fine.

Our subject matter today is an issue of great importance on breaches of data security involving the invasion of privacy. The statistics show that—you can start to run the clock now that I am on the subject matter. I adhere to the strict time limits myself.

The statistics show that there were 10 million victims of identity theft and identity fraud in the year 2003, at a cost to those individuals of some $5 billion, $50 billion in business losses; very extensive participation by the Government on data, with the Department of Justice having paid some $75 million to ChoicePoint last year on data processing.

We are in a field of phenomenal electronic advances. Chief Justice Warren was prescient back in 1963 in a decision on *Lopez* v. *United States*, saying that, quote, "The fantastic advances in the field of electronic communications constitute a great danger to the privacy of the individual." And where we have moved from 1963 is enormous and we now see the breaches in security and it is a matter of serious consequences for our individual privacy and also for law enforcement, which is relying upon these electronic mechanisms to identify suspects and pursue legitimate law enforcement interests.

There has been an entire industry which has grown up on this subject providing very, very important services, having databanks which enable applicants for mortgages to get them the same day, applicants for leases on apartments to get them the same day, credit card applications being processed, so that it has facilitated our lives, but it has had the corollary problem of the invasions of privacy.

There has been limited governmental response. Some States have laws. There is no Federal legislation on the issue. The United States General Accounting Office reports that, quote, "Criminal law has thus far proven to be quite ineffective in grappling with identity theft in that States devote insufficient attention and resources to prosecuting identity theft." The major companies who are represented here today—ChoicePoint, LexisNexis and Acxiom—have personal data on millions of Americans, including the identity as to name, address, Social Security numbers, insurance claims history, credit history, vehicle ownership, military service, educational history, outstanding liens or judgments, fingerprints, and even DNA. So it is a very, very wide array of information which is available.

There is no Federal legislation on the subject, and after the review for this hearing it is my conclusion that we do need Federal legislation, that there needs to be uniformity as we approach an enormous problem of this sort.

I took about a minute before the clock went on, so I am going to stop at this juncture and yield to my distinguished ranking member, Senator Leahy.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. That is a hint for the ranking member not to go overly long, too, but I want to thank the Chairman for doing this hearing. I wrote to him earlier this year and asked that we do it. I know that we both share this concern about privacy and this helps a great deal.

I am glad to see Senator Feinstein here, who has been a leader on this, and Senator Schumer and other members of the Committee, and Senator Nelson from Commerce. I am glad to see a fellow Vermonter, Bill Sorrell, who is the Attorney General of Vermont and President of the National Association of Attorneys General.

I think of all the major security breaches involving large firms such as ChoicePoint, Bank of America and Seisint, a LexisNexis subsidiary, and it shows the susceptibility of our most personal

data to relatively unsophisticated scams. These are not major things where somebody went in with some major, high-tech hacking. This was something where they used basically con games and got so much of this information.

It raises broader concerns, like industry's failure to know its own customers by properly screening the buyers of consumers' data. Advanced technology, combined with the realities of the post-9/11 digital era, have created strong incentives and opportunities for collecting and selling personal information about each and every American. Every single American in this room, as well as every American throughout the country—there is an incentive to collect the data about them and then to sell it.

All types of corporate entities routinely traffic in billions of digitized personal records to move commerce along. Our Government is using it now to know its residents. There is a certain Orwellian twist to this. I can make a lot of arguments of why business needs it, but I can also make a strong argument why if business is not careful with their trust or Government is not careful with their trust, we Americans are severely damaged and the country is severely damaged. Our privacy and our security is damaged.

Increasingly, those who trade in data have no direct relationship with the individuals and faces behind the numbers or letters that identify them. So the normal market discipline of disgruntled consumers does not save the companies from themselves.

We had one major company that sent the most personal data about their consumers on an airplane just to ship it off to another area. All of us who fly very much, we know our suitcases get lost. This was a case, and they were cavalier about that, where they just sent it out, showing absolutely no concern for their customers. And then I read in the paper two days ago that their former president is given, even though he is retired, lifetime use of the corporate jet. No wonder they treated it so cavalierly. They don't have to worry about lost luggage. If they did, maybe they would be concerned about the lost data of their customers. Frankly, if I were a customer of that company, I would change companies.

The case of Amy Boyer is a poignant reminder. In 1999, a man who had been obsessed with her since high school bought Amy's Social Security number, work address and other information from data broker Docusearch for $154. He used that information to track her down, and one day as she was leaving work he fatally shot her just before killing himself. For $154, he could track her down.

For others, inaccurate or misused data has meant job refusals or in many cases a life-consuming cycle of watching their credit unravel and undoing the damage caused by security breaches and identity theft. Individuals working for an Indian data processor stole personal information of Citibank customers, along with $350,000 just to make it worthwhile.

Last year, a Pakistani transcriber of medical files from a San Francisco hospital threatened to post that information on the Internet unless she received back pay. We outsource this to other countries anyway. They are holding our information in other countries and if they want to blackmail us with it, there is not much we can do.

I think weaknesses in the data industry can jeopardize our law enforcement and our homeland security. Government contracts that provide critical data and processing tools have to get it right. Our hearing today is not about shutting down these data brokers or abandoning their services. It is about shedding a little sunshine on current practices and weaknesses, and frankly, in my estimation, some very, very sloppy, sloppy business practices by some of these companies, and then to establish a sound legal framework to ensure that privacy, security and civil liberties will not be pushed aside.

Industry leaders like ChoicePoint, Acxiom and LexisNexis play a legitimate and a valuable role in the information economy. But because they are so valuable, they also need to treat these more carefully.

I will put the rest of my statement in the record, Mr. Chairman, but I am extremely concerned that we are not protecting customers and consumers around this country in the way we should. The companies get the benefit of having the data, but they also have a responsibility. We have to also consider some of the privacy issues that should affect every single one of us.

Chairman SPECTER. Without objection, Senator Leahy's full statement will be made a part of the record, as will my full statement.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman SPECTER. We turn now to a distinguished member of this panel who has taken initiative in introducing legislation in the field, as has Senator Schumer and some other Senators, but I think Senator Feinstein has put in the lead legislation, with some substantial experience from her home State of California.

We are going to waive the oath for you, Senator Feinstein, but everybody else is going to be put under oath.

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

Senator FEINSTEIN. Thank you very much, Mr. Chairman, and because you referred to what you have been going through in your opening statement, I just want to say how much personal respect I have for you for doing what you are doing in the way in which you are doing it. You have been an extraordinarily fair Chairman and this Senator really appreciates it. I think your vigor and your ability to carry out this work is truly amazing.

Chairman SPECTER. Thank you very much. Thank you.

Senator FEINSTEIN. You are welcome.

Chairman SPECTER. Start Senator Feinstein's clock at five minutes.

Senator FEINSTEIN. Thank you.

[Laughter.]

Chairman SPECTER. And anything else she may care to say about me, we will restart it at five minutes, so long as it is similarly laudatory.

Senator FEINSTEIN. Thank you very much.

I think most people don't understand that when they shop, when they buy a car, when they buy a home, what they buy, when they

buy out of a catalog, when they use a credit card, all bits and pieces about their personal data are collated and put together—their Social Security number, their driver's license, their personal financial data, their personal health data.

And it is used; it is used by banks who sell to subsidiaries. I am told Citibank sells to 2,000 different companies. There are companies that put this data together that are here today that also sell it, and the individual has no knowledge of this, has not given their permission, knows nothing about it, until one day they are a victim of identity theft.

And this is not a small thing. There were 9 million victims this last year alone. Of the 12 big breaches of databases that took place this year and during last year, the personal data of 10.7 million Americans has been put in jeopardy of identity theft. That is where we are going. It is huge and it is large.

This is the third Congress in which I have introduced bills, bills to give an individual some control. You have to give your permission before your personal data is sold. That is called opt-in. For less personal data, it is opt-out. To restrict use of Social Security numbers, to require that they be redacted from public documents—that is a second bill, and so on.

This bill, S. 115, is patterned after the California law. We would not have known of these breaches had it not been for California law. As a matter of fact, I am told that ChoicePoint—and I am sure if this is not correct, they will say so when they testify—had a prior breach and didn't notify anyone until the California law required them to notify Californians, and then others protested and they notified more people. So we have a bill that follows California law.

On Monday, I introduced a new bill after working with consumer advocates to broaden the scope, and the new bill's number is 751. This bill will ensure that Americans are notified when their most sensitive personal information—their Social Security number, their driver's license or State identification number, their bank account and credit card information—is part of a data breach, putting them at risk of identity theft.

This bill would require a business or government entity to notify an individual in writing or e-mail when it is believed that personal information such as a Social Security number, driver's license, credit card number has been compromised. Only two exceptions exist: first, upon the written request of law enforcement—that is obviously pending an investigation—for purposes of criminal investigation, and, second, for national security purposes.

The bill is based on California law, but California law really opened our eyes to the breadth and depth of the problem. This bill covers both electronic and non-electronic data, as well as encrypted and unencrypted data. California law only includes unencrypted electronic data.

This new bill would allow individuals to put a seven-year fraud alert on their credit report. The California law doesn't address fraud alerts. It doesn't include a major loophole allowing companies to follow weaker notification requirements, as the California law does. Our bill lays out specific requirements for what must be included in notices, including a description of the data that may have been compromised, a toll-free number to learn what information

and which individuals have been put at risk, and the numbers and addresses for the three major credit reporting agencies. By contrast, California law is silent on what should be in notices.

This bill has tougher civil penalties—$1,000 per individual they fail to notify, or not more than $50,000 a day while the failure to notify continues or exists. In California, a victim may bring a civil action to recover damages or the company may be enjoined from further violations. And most importantly, this bill sets a national standard so that individuals in Iowa, Oklahoma and Maine have the same protection as consumers in California.

The law would be enforced by the Federal Trade Commission or other relevant regulators, or by a State attorney general who could file a civil suit. And because the bill is stronger than California law, leading privacy groups, including Consumers Union and Privacy Rights Clearinghouse, have endorsed this legislation.

I would like, if I might, to put these letters in the record, Mr. Chairman.

Chairman SPECTER. Without objection, they will be made part of the record.

Senator FEINSTEIN. I would like to end with one case that I think depicts what has happened. You can't tell the true impact of identity theft by looking at numbers. Let me give you the case of Rebecca Williams. She lived in San Diego in 2000. A thief was using her Social Security number, her birth date and her name to establish a parallel identity thousands of miles away in the Chicago area.

The thief opened a phone line and utilities, obtained a driver's license and signed up for credit cards in her name. He even tried to use her identity to purchase a car. In all, the thief used Ms. Williams' identity to open more than 30 accounts, accruing tens of thousands of dollars' worth of goods and services. Sometimes, accounts were opened despite the fact that fraud alerts had been issued.

Ms. Williams said that restoring her identity is like a full-time job, and estimates that she spent the equivalent of eight hours a day for three full months working with credit bureaus, credit card companies and various government agencies.

Chairman SPECTER. Senator Feinstein, I note you have considerably more text. Could you summarize?

Senator FEINSTEIN. I certainly will. The point is that five years later, she has not fully restored her identity. That is how serious this is.

So I thank you for holding this hearing, and I would ask that my full statement be entered into the record.

Chairman SPECTER. Without objection, it will be made a part of the record in full. Again, thank you, Senator Feinstein for your leadership and your early leadership in this field.

[The prepared statement of Senator Feinstein appears as a submission for the record.]

Chairman SPECTER. We are going to start the hearing today with a video demonstration on what the impact is of knowing someone's Social Security number. We all know that the Social Security number is an entry point to a great deal of information about people, and we similarly know that we are frequently asked to give our So-

cial Security number in contexts where we question the necessity for it. It may well be that Congress will consider prohibitions against disclosure of Social Security numbers and some very heavy tightening up of this very basic point of identification which we all necessarily have.

We have with us Mr. Robert Douglas, who is the CEO of PrivacyToday.com. His full background will be made a part of the record, but in the interest of brevity I want to turn to him right now for his video demonstration.

STATEMENT OF ROBERT DOUGLAS, CHIEF EXECUTIVE OFFICER, PRIVACYTODAY.COM, STEAMBOAT SPRINGS, COLORADO

Mr. DOUGLAS. Thank you, Chairman Specter, ranking member Leahy, distinguished members of the Committee. My name is Robert Douglas.

Chairman SPECTER. Excuse me. Do you have similar screens for Senator Feinstein and Senator Feingold so they can follow this?

Senator FEINSTEIN. It is right over there.

Chairman SPECTER. Can you see it?

Senator FEINSTEIN. No, but it is there.

[Laughter.]

Chairman SPECTER. Let the record show it is there.

Proceed, Mr. Douglas.

Mr. DOUGLAS. We do have hard copies of these available for the members.

My name is Robert Douglas. I have been a private investigator and security consultant for the last 22 years, the last 8 years of which I have specialized in identity crimes and fraud. This is my fifth appearance before the United States Congress testifying on these types of crimes.

I have provided expert testimony to the Federal Trade Commission in Operation Detect Pretext, the Florida statewide grand jury on identity theft, and on the murder case of Amy Boyer that Senator Leahy—

Chairman SPECTER. Your credentials as an expert are taken. On to the issue.

Mr. DOUGLAS. Thank you, sir. I have been asked to provide a brief demonstration of how it is to obtain a Social Security number, the other types of information that are available, and what harm can come from that information.

The first screen up is a website called SecretInfo.com, which when asked by the Washington Post to obtain a Social Security of one of their reporters, I was able to do so on this search right here, locate a Social Security in 36 hours. I would note that from another company, U.S. Records Search, I received it in two hours telephonically.

To place the search online, all I did was go to the order page. I put in the name of the reporter, Jonathan Krim. I provided his current address, which we won't do for obvious reasons in the presentation here, and no other information. I scrolled down. I entered my name in the appropriate spot, entered my address information, which once again we won't share, and phone numbers that I could be contacted at.

I scrolled down a little further, provided a credit card number to make payment, hit the "I agree" button, and in 36 hours back came a very brief e-mail from Michael at SecretInfo.com providing the search results, the charge that had been applied to my credit card, the company that had applied the charge, and at the bottom Jonathan Krim, and obviously we have redacted his Social Security number for the presentation this morning. I would once again say that the other company, in two hours—they called me on my cell phone while I was driving home two hours afterwards.

This is another company that gives a very good example of the scope of the information that is available on the Internet—name and address information, phone record information, Social Security numbers, post office box—I would much of this already protected by Federal law—utility information, DMV information. I am sure the Senators are familiar with the Driver's Privacy Protection Act.

This is another search site that gives descriptions of the types of searches available. I would point out once again driving records, credit reports, and they often will have language that qualifies who they will sell this to. But the experience in the FTC operation when we called more than a hundred of these companies is if they trusted you, they would sell anything to anybody over the phone—credit card activity, including specific details of purchases; telephone records, including specific numbers that have been called; bank account information which, depending on how it is obtained, is in violation of Gramm-Leach-Bliley; airline travel records, which is a terrorist's dream.

Finally, I would like to just mention—and Senator Leahy mentioned the Amy Boyer case. That is the case that I worked on in New Hampshire. This is the firm that sold Amy's information, Docusearch.com. They are still in business today. In fact, Forbes magazine lists them as number one, and ChoicePoint is number two, of the firms that they recommend that people go to to buy information.

Why is that dangerous? In Amy's case, it ended up in this gentleman's hands, and I use the term "gentleman" quite loosely. This is Liam Youens standing in the corner of his bedroom with an AK–47. That is the gentleman that killed Amy Boyer once he bought her Social Security number, data of birth and place of employment.

That is the conclusion of my presentation, Mr. Chairman.

Chairman SPECTER. Thank you very much, Mr. Douglas. That is very informative.

We will now turn to our first panel—the Honorable Deborah Platt Majoras, Mr. Chris Swecker, Mr. Larry Johnson and Mr. Bill Sorrell. Would you all please step forward?

As a matter of practice, the Committee will swear in all witnesses. We are non-discriminatory. We had the Attorney General in last week and the Director of the FBI, so we want you to know that regardless of rank, station, et cetera, we think this is a preferred policy.

If you would all rise and raise your right hands, do you swear that the testimony you will provide to the Senate Judiciary Committee will be the truth, the whole truth and nothing but the truth, so help you God?

Ms. MAJORAS. I do.

Mr. SWECKER. I do.
Mr. JOHNSON. I do.
Mr. SORRELL. I do.
Chairman SPECTER. May the record show that all of the witnesses answered in the affirmative.

Our first witness is the Honorable Deborah Platt Majoras, Chairman of the Federal Trade Commission. Prior to her service at the FTC, she practiced law with the prestigious firm of Day Jones in Washington. In 2001, she was appointed Deputy Assistant Attorney General for the Antitrust Division, and Principal Deputy in 2002. She has an excellent academic record, summa cum laude from Westminster and a law degree from the University of Virginia.

Thank you for joining us, Madam Chairman, Madam Chairwoman, Madam Chairperson, and you have five minutes. We look forward to your testimony.

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

Ms. MAJORAS. Thank you very much, Mr. Chairman, ranking member Leahy, Members of the Committee. I am Deborah Majoras, Chairman of the Federal Trade Commission. I am grateful for the opportunity to testify today about securing personal information collected by data brokers and reducing the risks of identity theft.

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

Recent revelations about security breaches that resulted in disclosure of sensitive personal information about thousands of consumers have put the spotlight on data brokers like ChoicePoint and LexisNexis which collect and sell this information. This data broker industry includes many types of businesses providing a variety of services to an array of commercial and government entities.

The information they sell is used for many purposes, from marketing to assisting in law enforcement. Despite the potential benefits of these 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 the FTC is well aware, identity theft is a pernicious problem. Our 2003 survey estimated that almost 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing consumers $5 billion in out-of-pocket losses and American businesses $48 billion in losses.

The survey looked at two major categories of identity theft—the misuse of existing accounts and the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims in both time and money spent solving the problem. So, of course, people who had new accounts opened in their names, while they made up only one-third of the victims, nonetheless suffered two-thirds of the direct financial harm. Our survey also found that victims spent

almost 300 million hours correcting their records and reclaiming their good names. That is a substantial toll and we take seriously the need to reduce it.

There is no single Federal law governing data brokers. There are, however, some statutes and regulations that address the security of access to the information they maintain, depending on how the information is collected and 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 need for the information. Similarly, the Gramm-Leach-Bliley Act imposes restrictions on the extent to which financial institutions may disclose consumer information related to financial services and products.

Under that Act, the Commission issued its Safeguards Rule, which imposes security requirements on a broadly defined group of financial institutions that hold customer information. The Commission recently brought two cases in which we alleged that the companies there had not taken reasonable precautions to safeguard consumer information.

Finally, Section 5 of the FTC Act prohibits unfair or deceptive practices by a broad spectrum of businesses, including those involved in the collection and use of personal information. Using this authority, the Commission has brought a number of actions against companies that made false promises to consumers about how they would use or secure their sensitive personal information.

These cases make clear that an actual breach of security is not necessary for us to enforce under Section 5 if we determine that a company's security procedures were not reasonable in light of the sensitivity of the information the company maintains. Evidence of a breach, of course, however, may indicate that the company's procedures were not adequate, and our Commission staff monitors reports of breaches and initiates investigations where appropriate.

The Commission, consistent with the role Congress delegated in 1998, has worked hard to educate consumers and businesses about the risks of identity theft, as well as to assist victims and law enforcement officials. The Commission maintains a website and a toll-free hotline staffed with trained counselors to advise victims on how to reclaim their identities. We receive roughly 15,000 to 20,000 contacts per week on our hotline or through our website or from mail from consumers who want to avoid becoming victims and from victims themselves. The Commission also facilitates cooperation, information-sharing and training among Federal, State and local law enforcement authorities.

Although data brokers are currently subject to a patchwork of laws, depending on the nature of their operations, recent events raise the issue of whether these laws are sufficient. Although several alternatives have been proposed and we are considering each very carefully, the most immediate need is to address the risks to security.

One sensible step would be to mandate security requirements for sensitive personal information collected by data brokers much like the Commission's Safeguards Rule imposes on certain companies. It also is appropriate—

Chairman SPECTER. Chairman Majoras, could you summarize at this point?

Ms. MAJORAS. Yes, I will.

Finally, it is also appropriate to consider a workable Federal requirement for notice to consumers when there has been a security breach that raises significant risks to consumers.

Mr. Chairman, members of the Committee, thank you very much. I look forward to working with all of you.

[The prepared statement of Ms. Majoras appears as a submission for the record.]

Chairman SPECTER. Thank you.

We turn now to Mr. Chris Swecker, who is the Assistant Director of the Criminal Division of the Federal Bureau of Investigation. Mr. Swecker has a very extensive background in field work, has been with the FBI since 1982. His academic record is a bachelor's degree from Appalachian State University and a law degree from Wake Forest. He also served as—this is the highlight of your resume, Mr. Swecker. You were an assistant district attorney. People sometimes ask me what is the best job I ever held and expect to hear Senator, maybe D.A. And I say, no, assistant D.A.

Start the clock at five minutes for Mr. Swecker.

STATEMENT OF CHRIS SWECKER, ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Mr. SWECKER. Good morning, Mr. Chairman and members of the Committee. I want to thank you for the opportunity to testify today on the FBI's efforts to combat identity theft, as well as the FBI's use of public source data.

The FBI views identity theft as a significant and growing crime problem, especially as it relates to the theft of consumer information from large wholesale data companies. The FBI opened 1,081 investigations related to identity theft in fiscal year 2003, and 889 in fiscal year 2004. I might add that a case that involves the theft of 1,000 identities would only be counted as one investigation within the FBI's structure.

That number is expected to increase as identity thieves become more sophisticated and as the technique is further embraced by large criminal organizations, placing more identity theft crime within the FBI's investigative priorities. At present, we have over 1,600 active investigations involving some aspect of identity theft.

The FBI does not specifically track identity theft convictions and indictments, as identity theft crosses all program lines and is usually perpetrated to facilitate other crimes such as credit card fraud, check fraud, mortgage fraud and health care fraud.

Armed with a person's identifying information, an identity thief can open new accounts in the name of a victim, borrow funds in the victim's name, or take over and withdraw funds from existing accounts of the victim, such as their checking account or their home equity line of credit. Although by far the most prevalent, these financial crimes are not the only criminal uses of identity theft information, which can even include evading detection by law enforcement in the commission of violent crimes.

Identity theft takes many forms, but generally includes the acquiring of an individual's personal information such as Social Security number, date of birth, mother's maiden name, et cetera. Identity theft has emerged as one of the dominant white collar crime problems of the 21st century. Estimates vary regarding the true impact of the problem, but agreement exists that it is pervasive and growing.

In addition to the significant monetary harm caused to the victims of the frauds, often by providers of financial, government or other services, the individual victim of the identity theft may experience a severe loss in their ability to utilize their credit and their financial identity.

In a May 2003 survey commissioned by the FTC, they estimated that the number of consumer victims of identity theft over the year prior to the survey at 4.6 percent of the population of U.S. consumers over the age of 19, or 9.9 million individuals, with losses totaling $52.6 billion. Half of these individuals experienced the takeover of existing credit cards, which is generally not considered identity theft. New account frauds, more generally considered to be identity theft, were estimated to have victimized 3.23 million consumers and to have resulted in losses of $36.7 billion.

The FBI's Cyber Division also investigates instances of identity theft which occur over the Internet or through computer intrusions by hackers. The Internet Crime Complaints Center, also known as IC3, is a joint project between the FBI and the National White Collar Crime Center. This joint collaboration serves as a vehicle to receive, develop and refer criminal complaints regarding the rapidly expanding arena of cyber crime.

The IC3 receives an average of 17,000 complaints every month from consumers alone, and additionally receives a growing volume of referrals from key e-commerce stakeholders. Of the more than 400,000 complaints referred to IC3 since its opening in May of 2000, more than 100,000 were either characterized as identity theft or involved conduct that could be characterized as identity theft.

The FBI is developing cooperative efforts to address the identity theft crime problem in cities such as Detroit, Chicago, Memphis and Mobile. Task forces are currently operating in conjunction with our other State, Federal and local partners.

An example of some of the cases involve a case involving, in September 2004, Phillip Cummings in the theft of over 30,000 consumer credit histories from 2000 to 2002. Losses to financial institutions in this case exceeded $11 million. He was sentenced to 14 years in Federal prison.

In January of 2003, another case involved the theft of over 100 credit reports by someone posing in the account name of NEXTEL. The cases go on and on. I won't belabor you with all of the different investigations. There is a case, as you well know, involving ChoicePoint, where there wasn't an IT intrusion. It was actually a socially-engineered con effort, as Senator Leahy pointed out, involving a customer who used over 23 business identities to access accounts through ChoicePoint.

Chairman SPECTER. Mr. Swecker, your red light is on. Time has expired. If you could summarize at this point, we would appreciate it.

Mr. SWECKER. ChoicePoint information is not considered in a vacuum. It is one of the many investigative tools which are used in law enforcement by investigators and analysts. As with any source of information, it is considered in relation to the totality of available information. It is particularly useful in that it allows analysts to inductively and deductively develop information about subjects, their confederates, witnesses and corporations that are associated with an investigation.

Once again, I appreciate the opportunity to come before you today and share the work that the FBI has undertaken involving identity theft. The FBI's efforts in this arena will continue and we will continue to keep the Committee informed of our progress.

[The prepared statement of Mr. Swecker appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Swecker.

We turn now to Mr. Larry Johnson, who is the Special Agent in Charge of the Criminal Investigative Division of the Secret Service. Mr. Johnson is a 20-year-plus veteran of the Secret Service, having started in 1982. He has worked in quite a number of field offices around the country and was the Assistant Special Agent in Charge of the Presidential Protective Division. He has a bachelor's degree from Eastern Kentucky.

Thank you very much for joining us, Mr. Johnson.

STATEMENT OF LARRY JOHNSON, SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE, WASHINGTON, D.C.

Mr. JOHNSON. Thank you, Mr. Chairman. In addition to providing the highest level of physical protection to our Nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment system, the Secret Service has a long history of protecting American consumers and industry from financial fraud.

With the passage of Federal laws in 1984, the Secret Service was provided primary authority for the investigation of access device fraud, including credit card, debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases.

In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically. With the expanding use of the Internet and lower cost of information processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokering.

Information collection has become a common by-product of newly emerging e-commerce. Internet purchases, credit card sales and other forms of electronic transactions are being captured, stored and analyzed by businesses seeking to find the best customers for their products.

This has led to a new measure of growth within the data collection industry that promotes the buying and selling of personal information. In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on

the Internet. They may not realize that the information they provide in credit card applications, loan applications or with merchants they patronize are valuable commodities in this new age of information trading.

This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom will organize and operate across international borders. But legitimate businesses can provide a first line of defense against identity crime by safeguarding the information they collect. Creating industry standards in this area can significantly limit the opportunities for identity crime even while not limiting its occurrence altogether.

With the proliferation of computers and the increased use of the Internet, high-tech identity criminals began to obtain information from company databases and websites. In some cases, the information obtained is in the public domain, while in others it is proprietary and is obtained by means of computer intrusion or by means of deceptions such as Web spoofing, phishing and social engineering.

The method that may be most difficult to prevent is the theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment. This collusive employee will access the proprietary database, or copy or download the information or remove it from the workplace either electronically or simply by walking it out.

The Secret Service has seen Internet crime increase significantly within the last several years. Since the early 1990s, the Eurasia-based computer underground in particular has developed a prodigious record for malicious software development. Starting in the late 1990s and increasing over the last few years, the criminal element has used such malicious software to penetrate financial and government institutions, extract data and illicitly traffic in stolen financial identity information. We believe that the exploitation of identity theft information is primarily for financial purposes.

I would like to talk briefly about agency coordination and criminal sophistication. It has been our experience that criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as first responders to criminal activity.

By working closely with other Federal, State and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence-sharing, resource-sharing and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Chairman SPECTER. Mr. Johnson, your time is expired. If you would summarize, we would appreciate it.

Mr. JOHNSON. Finally, the best example of agent coordination was on October 24, 2004, when the Secret Service arrested 30 individuals across the United States and abroad for credit card fraud. The suspects were part of a multi-count jurisdiction investigation out of the district in New Jersey. We had 30 arrests, 28 search warrants served simultaneously not only in the United States, but in 11 different countries throughout the world in conjunction with this investigation.

Thank you.

[The prepared statement of Mr. Johnson appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Johnson.

I note that there are still some people in the hall. If there are, you ladies and gentlemen are welcome to move into an area here where we have some space. Are there others who are still in the hall without being able to come into the hearing room? We don't want anybody to miss our hearing. Well, if anybody comes, they are welcome to come, and if you folks would move over into some open space to give some room, we would appreciate it.

I want to turn now to the distinguished ranking member to introduce his home State attorney general.

Senator LEAHY. Well, thank you, Mr. Chairman. I am glad to have Bill Sorrell here. He has been Attorney General of Vermont since May of 1997—that is an elective office—first appointed when the then attorney general went on to become chief justice of the State. In elections, he has ended up being basically endorsed by both parties. While everybody else worries about reelection, he just sort of walks in with the strong support of all Vermonters.

But I mention that, really, before being attorney general he held the best elected job that there has ever been in the State of Vermont, and that is he was Chittenden County State's attorney. Anyone who has been Chittenden County State's attorney will tell you that there is no finer job that you could have in the State of Vermont, even the United States Senate. So I am glad he is here. He is now President of the National Association of Attorneys General, and I think we are fortunate to have him here with us. I thank you, Mr. Chairman, for inviting him.

Chairman SPECTER. Welcome, Mr. Sorrell. Were you ever an assistant prosecutor?

STATEMENT OF WILLIAM H. SORRELL, ATTORNEY GENERAL, STATE OF VERMONT, AND PRESIDENT, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, MONTPELIER, VERMONT

Mr. SORRELL. I was, yes, and that was a great job, too.

Chairman SPECTER. Thank you for joining us and the floor is yours.

Mr. SORRELL. Thank you, Mr. Chairman, Senator Leahy, and other members of the Committee, for giving me the opportunity to be here and talk about some issues that are of great importance to me and my fellow attorneys general.

I am the President of the National Association of Attorneys General, and I am confident that most of my colleagues, if not all—and it could be all—agree with the thoughts that I will present today.

But I would ask the Committee to consider that these are my remarks as the Vermont Attorney General.

First of all, I want to start, Senator Feinstein, by thanking California for enacting the disclosure law. But for that law, ChoicePoint might not have disclosed the security breaches. We might not have seen and had the scrutiny we have on these issues. We might well not be here today. So my thanks.

In thinking about my remarks today, I was reminded of the quote that is attributed to the famous bank robber Willie Sutton. Asked why he robbed banks, he said that is where the money is. Unlike the days perhaps when Senator Leahy and I were county prosecutors and you were worried about losing your TV or your stereo and maybe your money, these days where the money is is in the computers of data brokers, credit reporting agencies and other large financial institutions, academic institutions and the like, the personal information that they have, because if they can gain that personal information, they can not only drain your finances from the accounts that you have, but more importantly, and in the case of so many Americans, more than the value of what they have in accounts is their access to credit. What identity theft is about in many, many cases is stealing one's access to credit.

I am maybe dating myself a bit, but five or so years ago I was here in D.C. speaking to one of the Senate committees on Gramm-Leach-Bliley issues and saying at that time that with the way the economy was changing, with the ability to collect more and more information, we might well have been looking back on that time someday and saying that was the good old days when privacy was privacy.

Well, here we are today and we see that more information is being gathered and that clever criminals are finding more and more ways to steal from us, to the tune of what the Chair of the FTC indicated to be $50 billion a year, and that number going up.

We are here to say that the time for Federal action is now. We much appreciate the fact several bills are being considered in this area of the importance of the privacy and protection of our personal information. We hope that the Congress will follow the lead of California, and now up to 30 States that are considering disclosure laws, to enact a security breach notification law.

To the extent that you can take into account the fact that the quicker the notification goes out to consumers that their personal information has been accessed, then the FTC studies show rather dramatically that the amount of the loss can be significantly reduced. So time and effectiveness of the notice are of significant importance.

We ask you, if you enact such a law, to have your law be a floor rather than a ceiling in the same way under Gramm-Leach-Bliley the opt-out standard applies nationally. You have allowed States like Vermont to go forward and protect our citizens more and to adopt an opt-in standard if we wish. And we ask in this arena that you do the same thing, that you be respectful of the ability of the States; if the State wishes to be more protective, to be able to do so.

The Chair indicated that the regulation of data brokers is sort of piecemeal. We ask you to pass a Federal statute that regulates

data brokers, again, not to preempt the States with whatever you might do. Finally, we ask you to strengthen the safeguards rules under Gramm-Leach-Bliley and to include in those safeguard rules data brokers. We trust and hope that you will remain mindful and appreciative of the role that the States have played both legislatively and in investigations in this area of personal information, the importance of it, and we look forward to working with you going forward.

Thank you for asking me to be here today.

[The prepared statement of Mr. Sorrell appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Attorney General Sorrell.

Senator Coburn has appropriately noted that some of the testimony was submitted late, and we are going to be enforcing a strong rule that where testimony is not submitted in time, then witnesses will not be permitted to make opening statements, but only to respond to questions, because it is very important that we get that on time. There is a tremendous amount of work to do to collate these materials and I thought that cautionary word would be in order at this time.

Thank you, Senator Coburn, for focusing on that.

Senator LEAHY. Mr. Chairman, I have a question on that. What do we do in those cases where testimony is submitted, but then entirely different testimony is given? I am thinking, for example, of the Attorney General the other day submitted testimony, but then the testimony he gave was considerably different. I wouldn't to preclude him.

Chairman SPECTER. Well, that happens from time to time and leads to more vigorous cross-examination. I heard you, Senator Leahy. He paid the price by offering different testimony from what he had submitted in writing.

Senator LEAHY. Thank you.

Chairman SPECTER. I don't think there is any way you can control that. If people have to submit testimony, they will have to focus on it and we will have at least that advanced notice. But I do agree with you that it is problemsome when you have something new that you haven't been prepared for, but I thought you handled it very adroitly.

Senator LEAHY. We are talking about the U.S. Attorney General, not the Vermont Attorney General.

Mr. SORRELL. I understand that. Thank you.

Chairman SPECTER. Each member will now have five minutes on questioning, and I would ask that the responses be brief.

Starting with you, Madam Chairwoman Majoras, what kind of Federal legislation would you like to see?

Ms. MAJORAS. Well, as I said briefly in my opening statement, Senator, we think that looking at extending our GLB Safeguards Rule across a broader spectrum of companies so that companies are required by law to have in place security measures would be a terrific first step. And as a second step, we think we ought to look at notice provisions where consumers are at risk from breaches.

Chairman SPECTER. Well, we will be submitting to you the draft legislation we have. You have had a lot of experience in the FTC.

I want to address a question to both Mr. Swecker and Mr. Johnson. Both the FBI and the Secret Service has contracted out; the FBI paid about $75 million last year. What are you doing, Mr. Swecker, to guarantee the security of information which is so critical to law enforcement?

Mr. SWECKER. Well, the existence of our queries by contractor are not known—I mean, the existence is known, but the substance of the queries are not known to ChoicePoint or any of the data brokers that we contract with. They collect the number and other information, but they do not collect the subject of the query.

Chairman SPECTER. Are you saying then that the security breaches like we have seen do not impact on the FBI and the security of the information that you deal with?

Mr. SWECKER. Not in the sense of knowing who we have initiated queries on. That data, ChoicePoint and other data brokers tell us, is not collected by them, only the number of queries and some other basic information for billing purposes.

Chairman SPECTER. From the point of view of the Secret Service, Mr. Johnson, do you face any security problems on breaches that we have seen here?

Mr. JOHNSON. Mr. Chairman, no, we have not. In similar form and fashion with the FBI, that is not known to the broker. Other things that the Secret Service does is we continuously monitor the information. We have assessment teams only looking at the information flow to see if we are vulnerable in any aspect of the information being leaked.

Chairman SPECTER. Attorney General Sorrell, you have testified that you would not like to see the State laws preempted. We have now many States which have legislated in the field and we are considering Federal legislation. You have these companies which will have to comply with a patchwork of legislation.

There has been some thought that this ought to be a matter for Federal jurisdiction on lawsuits, and at least at this point I have grave reservations about that, first, because the Federal courts are so heavily burdened at the present time. And, secondly, if you come from a rural part illustratively of Pennsylvania, Fulton County, you don't want to go to Harrisburg or Pittsburgh to litigate your case. You can litigate Federal claims in the State court.

I would like you to address the two issues. First, why not preempt State laws so that these companies know what they are dealing with and don't have to familiarize themselves with the many, many differences?

Mr. SORRELL. First of all, Senator, on this idea of a patchwork of different laws, our economy, with globalization, is becoming a world economy so that there are clearly differences between countries. We have some States which have economies larger than most of the countries of the world, and since we are talking about computers and information, it is really more of a system of programming.

I mentioned Gramm-Leach-Bliley. We have for our insurance and financial services and banking industry in Vermont an opt-in standard rather than the national opt-out standard. Our Vermont economy has not suffered. Companies want to come in and do business there. It is doable and it is a minimum burden to become

aware of the level of laws in each of the States and to stay in compliance with that.

Roughly 30 of the States are looking at disclosure laws now and many of the States are looking at the security freeze laws. These same companies are very mindful of what is going on in the State houses and are in there lobbying. They want a single standard which would be easier for them. But in our view, in Vermont, Vermonters, if they want to go further, should be allowed to do so.

Chairman SPECTER. My time has expired and I will yield at this point to Senator Leahy.

Senator LEAHY. Well, thank you, Mr. Chairman.

Madam Chair, we talked about ChoicePoint, LexisNexis, and so on. These are well-known, but there are a whole lot of other companies that operate well beneath the radar. Some get even more involved in our personal life and data.

Does the FTC have any current plans to examine, identity and check these other industry players?

Ms. MAJORAS. Senator Leahy, the FTC has been interested in this industry for some time, since before the recent revelations that have been in the news. We are working hard to try to get a better handle on this industry. It is hard to know at this point whether we can even call it just an industry because it seems to have many facets, depending on how you define it.

So in addition to several investigations that we have pending, we are, in fact, trying to get our arms around who the players are here so that when we are working in law enforcement and when we are asked by Congress to help with possible legislation, we have the facts and we know what it ought to pertain to.

Senator LEAHY. Some of the privacy experts suggest applying some kind of fair information practices, something similar to the Fair Credit Reporting Act, to the data brokers that are not currently subject to such similar protections. Would you support such an application?

Ms. MAJORAS. I think we should look at whether some of those provisions should be applied. For example, if we have a data broker who is collecting information with respect to marketing practices, consumers, for example, may not care very much about the accuracy of that information that is being collected. So that may be an area where consumers don't even want to be bothered with checking the accuracy. So again we want to make sure that if we extend these, we extend them in a way that makes sense.

Senator LEAHY. Thank you, and I may have my staff follow up a little bit with yours on that subject.

Ms. MAJORAS. Yes, sir.

Senator LEAHY. Mr. Swecker, just to follow up a little bit on what the Chairman was asking you, has the FBI audited any of the commercial data brokers with whom you have contracts to evaluate how they comply with those contracts and security products? I am thinking insofar as you use them sometimes for criminal searches.

Mr. SWECKER. No, Senator, we have not done a formal audit. We have looked at their protocols and how they capture our queries and the substance of the query is not captured. The way it is explained to me is there is a logging protocol that is used that masks the existence or the substance of our query, but does capture other

information just simply for their billing purposes, but no formal audit.

Senator LEAHY. And none planned?

Mr. SWECKER. I am sorry, sir?

Senator LEAHY. And none planned that you know of?

Mr. SWECKER. None planned that I know of.

Senator LEAHY. We may want to follow up further on that with you.

We also have the whole question of data mining technology. There are a lot of different forms of it, algorithms that look for patterns, profiles, and so on. What kind of data mining does the FBI utilize, and assuming you can answer this in an open hearing, what kinds of protections are in place to prevent abuse?

Mr. SWECKER. There really isn't data mining, per se. Each query is predicated and connected to an investigation, at least a preliminary inquiry. So we don't data-mine through the data broker's information. There are specific queries that are made that are connected to specific investigations that are predicated.

The closest that you could come to calling it data mining would be large-batch queries that are sometimes done with 40, 50 names at one time. But as far as just mining through the data, that does not occur.

Senator LEAHY. I will follow up with a further question on that.

Attorney General Sorrell, you said that many consumers in Vermont attempted to obtain a free report under Vermont law after learning about the ChoicePoint and the other security breaches. And they were told incorrectly, it turned out, by the credit bureau's voice mail systems that they were not eligible for a free credit report.

Have the credit reporting bureaus since resolved this problem? Have you heard from other attorneys general that they have had in their State the same kind of problem?

Mr. SORRELL. I think there are about seven States that, like Vermont, had a statute before the Federal statute granting individuals annual access to their credit reports. I haven't heard from the other States. We have communicated with the credit reporting agencies reminding them of the Vermont law, quite apart from the Federal law which, for Vermont, I don't think is effective until this coming September.

I don't have up-to-date information to know whether consumers have called in within the last couple of days to complain about that. But, again, this is one of those issues where Vermont and some other States were ahead of the Federal Government in setting a more protective standard for our consumers and the Congress followed suit, ultimately.

Senator LEAHY. Thank you. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Leahy.

Senator LEAHY. I have other questions I will submit for the record.

Chairman SPECTER. Fine.

Senator Coburn.

Senator COBURN. Thank you, Mr. Chairman.

Attorney General Sorrell, if we were to make changes in terms of trying to protect States' rights and States' options, can you sug-

gest a way to create an opt-in/opt-out phenomenon in the Bliley bill that would incorporate your concerns and still give you the flexibility as a State, but still we could have a more uniform practice throughout the country?

Mr. SORRELL. I would be happy to. This is really an area where I would be out in front of my colleagues, since we have not discussed an opt-in/opt-out national standard. I think it would depend on the nature of the information that is being collected and for what purposes it may be accessed; as the Chair suggested, marketing surveys as opposed to considerations for extension of credit and such.

One thing that a number of the States are doing right now which is very effective in terms of combatting identity theft is to be able to freeze access to your credit reports. California, Texas, Louisiana and Vermont have those laws or they are about to go into effect.

There is some downside for consumers when you do that because if you go to a store and want to open up an instant credit account, you can't get it. If you haven't thought a little bit ahead that you are looking for a mortgage to refinance or a new mortgage, or rent an apartment or buy a car or something like that, there is a time lag.

But on the other hand, when it is access to your credit that is the main way that you can be the victim of identity theft crimes, then you can put a hold on your credit history going out. Four States have done it and others are considering it, and it is a very effective tool that some of the States have looked at to combat identity theft. And you can do it for periods of time, you can do it on an ongoing basis, and it is much more effective than just putting a security alert on your credit history.

Senator COBURN. But for the State of Vermont and your position, you can't see that you would object if you were left with the flexibility to opt in or opt out for Vermont if we were to have Federal legislation?

Mr. SORRELL. I am sorry if I missed the point of your question, Senator. What I am asking for is that in this area of privacy, if there is Federal legislation that it be a floor as opposed to a ceiling and give the laboratory of the States, mindful of their priorities, the ability to be more protective if they wish, knowing that there might be some downside for individuals or for the economy in those States if they are willing to take on those burdens in return for the extra protection.

There is some burden for the companies to be dealing with different rules and regulations, but that is the case environmentally with any number of other consumer laws right now and it can be the case here.

Senator COBURN. Mr. Chairman, just for the record I would note that I have a great deal of difficulty with my credit card company because they are so aggressive, and as much as I travel around the country they won't let me charge until they talk to me on the phone. They are not sure I am who I think I am. Sometimes, I am not sure I am who I think I am.

But either way, we have a broad continuum of security checks that are going on now by individual businesses who offer credit, and I just think that the hearing ought to focus in the future on

how do we create a better climate for the security of consumers in terms of their credit, but also leave the States the individual right to opt higher. I would agree with you.

I thank you, Mr. Chairman.

Chairman SPECTER. Well, those are very important considerations, Senator Coburn. How do they tell it is you? Do they know your voice?

Senator COBURN. They ask for my mother's maiden name and my grandmother's maiden name.

Chairman SPECTER. You fellows from Oklahoma don't have such distinct dialects as those of us from Kansas.

Senator COBURN. We have a twang, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Coburn.

Senator Feinstein.

Senator FEINSTEIN. Well, thanks very much. Just quickly in response to Senator Coburn, the legislation that I have introduced in terms of protections for people in the opt-in/opt-out is that the opt-out is for significant personal data—Social Security number, driver's license, personal health, personal financial data. That would be opt-in. Lesser things would be opt-out. That is just for your information.

Attorney General, thank you very much for your comment about California. You mentioned that you thought this legislation should be a floor and not a ceiling, and that other States should be able to enter the arena. My concern is that if you have a different standard for notification—I am going to talk about that in a minute, but a different standard for notification in every State, it makes it very difficult.

It seems to me that the standard for notification should be the same; in other words, what kind of information you must notify on, what the procedures for notification are, can you do it in e-mail, must you do it in writing and e-mail. Those kinds of things should be national, and then anything a State wants to do in addition to that would be up to the State.

Could you comment?

Mr. SORRELL. Do you envision a standard of whether there is substantial likelihood of misuse of the information or that it is just notification that the information has been accessed?

Senator FEINSTEIN. Well, this is what I wanted to talk with the Chairman about because she has some quotes on this subject. I think any time the database is breached, that information is then out there. How do you know if it is significant risk, because somebody who gets 100,000 I.D.s about different people can sit back and use them in a year, in two years, can sell them? I think it is very difficult to determine significant risk.

Mr. SORRELL. I agree with you, Senator. I am pleased to hear you say that. I guess in answer to your other question, it depends on what standard you set. In the case of ChoicePoint, and with all due respect to ChoicePoint, it is my understanding that the notifications that they sent out originally to California and then, under some pressure or encouragement, to other Americans—these notices, or a number of them, when coming through the mail, came in envelopes that just said "ChoicePoint."

Now, frankly, I had never heard of ChoicePoint until this issue broke and if I had received something from ChoicePoint, I would have assumed it was just another credit card offer and it would have gone in the recycling bin. So, hopefully, to the extent that a Federal standard is set, the notification will be such that it will prominently let consumers know that this has to do with access to your personal information as opposed to something from a company maybe they never heard of.

Senator FEINSTEIN. Thank you. You have made a very good suggestion. We will take you up on it.

Good morning, Madam Chair. If I may, when you appeared before the Senate Committee on Banking, you stated in response to Senator Reed that prompt notification of breaches should be given when there is significant risk to consumers. I think this is one of the biggest areas in notice, the idea of what triggers notice so as to avoid over-notification, but at the same time ensure, just as I have pointed out, that individuals are notified because you don't know what might be done with that information. So I would like to explore this with you further.

I would like to know why you take the position that notice should only be sent if there is significant risk to consumers and how you would define that.

Ms. MAJORAS. Thank you. That is an excellent question, Senator Feinstein, and one that we are currently grappling with at the FTC. The issue is exactly the one that you have raised—over-notification. We have a lot of experience in dealing with consumers on a lot of different types of security issues and, of course, Gramm-Leach-Bliley, and what we have learned is that eventually consumers will become numb to notices if they are getting them consistently.

So, for example, when we have a young hacker who finds it to be sport to hack into a significant database and then call the company and say, "ha, ha," I hacked into your database, but who is then investigated and is seen not to have any intention, and indeed no longer has access to the information so that the person can commit the crime of identity theft, there isn't a risk there to consumers.

There are other types of situations we are envisioning in which, if we define breach very, very broadly, companies will have no choice but to be sending out constant notices to avoid liability. And we are worried that consumers will just think that it is a cry of wolf and will stop worrying about it. That is the concern.

Senator FEINSTEIN. I think your point is well taken if you have an opt-in/opt-out situation. Right now, consumers don't know; they don't know the depth and breadth. For example, the gentleman that ran the video—Senator Leahy pointed out health information is advertised on that website. They can get your hospital records. Now, how they do that I don't know.

Does anybody in this room want their hospital records sold or available to anybody? I don't think so, and that is where we are. So if we have for significant personal data the individual has to say, yes, Wells Fargo Bank, yes, ChoicePoint, yes, LexisNexis, you can sell my data, or you cannot sell my data, and for less signifi-

cant data that they must opt in, they must write a letter and I say I don't want any of my personal data sold for commercial profit—

Chairman SPECTER. Senator Feinstein, your time is a bit past.

Senator FEINSTEIN. It went by fast. Thank you, Mr. Chairman.

Chairman SPECTER. We are going to be starting a vote in just a few minutes. It has been advanced to 10:50 and I want to be sure we cover this round.

Senator Feinstein, have you concluded?

Senator FEINSTEIN. No, but my time is up.

Chairman SPECTER. Thank you.

Senator Feingold.

STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator FEINGOLD. Thank you, Mr. Chairman. I do want to thank you for holding this hearing today and I have benefitted from listening to the witnesses. I ask that my full statement be printed in the record.

Chairman SPECTER. Without objection, it will be made part of the record.

[The prepared statement of Senator Feingold appears as a submission for the record.]

Senator FEINGOLD. Thank you, Mr. Chairman.

I am concerned about an aspect of the data broker business that has not received a lot of attention. The information gathered by these companies is sold not just to individuals and businesses, but also to law enforcement agencies like the FBI. While the Government should be able to access commercial databases in appropriate circumstances, there are no existing rules or guidelines to ensure that this information is used responsibly, nor are there restrictions on the use of commercial data for powerful, privacy-intrusive data mining programs.

Mr. Chairman, that is why I am planning to reintroduce in the next few days my Data Mining Reporting Act which would require all Federal agencies to report to Congress on data mining programs used to find patterns, including terrorist or other criminal activity. I am glad this hearing gives us an opportunity to explore both government and commercial reliance on data brokers, and I look forward to working on Senator Feinstein's legislation and the other legislation that is being introduced to address this issue.

In terms of my time to question, Mr. Swecker, you testified that the FBI subscribes to some of ChoicePoint's products. No doubt that these databases are useful investigative tools and can in appropriate circumstances enhance the efficiency of investigations. But it would be helpful to understand more about how the Bureau uses information from companies like ChoicePoint.

So to begin, from what companies besides ChoicePoint does the FBI currently subscribe?

Mr. SWECKER. Senator, we contract with Dun and Bradstreet, LexisNexis, Westlaw, the National Insurance Crime Bureau, Credit Bureau Reports, as well. I think it is important to emphasize this is all publicly available information. It is just a compilation of public source information all in one place.

Twenty-three years ago when I first came to the FBI, I would have had to physically walk down to the courthouse to get courthouse records or go places to collect these records. Being able to make one query and get all these records at one time saves investigative time and it saves resources. That is why we use it. There is no data mining that takes place and I think that is—

Senator FEINGOLD. I am just trying to get some information first.

Mr. SWECKER. Okay.

Senator FEINGOLD. You mentioned in your testimony that ChoicePoint makes available public record information, but in an aggregated form. What type of public record information is contained in the products to which the FBI subscribes, and what other types of records are available to the FBI through commercial data brokers?

Mr. SWECKER. Everything from driver's license information, last known addresses, dates of birth, public court records, court filings, liens, newspaper records. It runs the whole gamut of public information.

Senator FEINGOLD. And then how often do investigators use these databases?

Mr. SWECKER. The data that I looked at showed that we conducted somewhere over a million inquires in 2003, I think, or close to a million, and possibly about 1.2 million, I think, just with ChoicePoint more recently, I think, in 2004. I may have my fiscal years mixed up there.

Senator FEINGOLD. Does the FBI have benchmarks regarding the accuracy and security of data that it uses to evaluate whether to enter into a contract with information brokers? Do you have a process to review the quality and the accuracy of the data?

Mr. SWECKER. My understanding is that is why we contract with all of these different companies because we are able to compare the information that comes in on the same person from four or five different data brokers and actually get to the accurate information. So that is why we don't just contract with one company. We contract with four or five different companies.

Senator FEINGOLD. But do you have a process to sort of compare and evaluate the quality of what you are getting? I mean, you are talking about contracting, you are talking presumably about spending the taxpayers' dollars to purchase this ability to do this. Is there an accountable and effective way to evaluate the quality and accuracy and security of this information?

Mr. SWECKER. Coming from the data brokers? We compare it to our own information as well and we have analysts that go through this data. Yes, of course, we try to make sure this is accurate information.

Senator FEINGOLD. Do you make determinations as to whether one is better than the other in terms of who you are going to contract with? I assume you make judgments that some are better than others.

Mr. SWECKER. Each one of these data brokers has a different strength in terms of what type of information they provide us and a lot of it is lead information that takes us somewhere else and it gives us places to start, comparing last known addresses, for example.

Senator FEINGOLD. Mr. Swecker, I understand from your testimony—I think Senator Leahy talked about this—that FBI agents use commercial databases to conduct individualized searches to locate people who are already suspects or to further an investigation of someone who is already a suspect. Actually, on this one I am interested in hearing from Mr. Johnson. I believe you already covered this.

Mr. Johnson, is the Secret Service also using commercial data to run more open-ended data mining searches to look for people who might fit a certain pattern of criminal or terrorist activity?

Mr. JOHNSON. We do. The way the Secret Service is, through partnerships and our electronic crimes task forces, most, if not all, data brokers are members of our task forces. So in conjunction with an investigation, they provide that small part of what we might need to further that investigation. Does that answer your question?

Senator FEINGOLD. So you use it, but you—

Chairman SPECTER. Senator Feingold, your time is expired. If you would conclude perhaps with another question—

Senator FEINGOLD. Thank you, Mr. Chairman. I am fine.

Chairman SPECTER. Senator Schumer has just joined us. His timing is impeccable. Economizing on his own time, he was here at the start and now comes right in when he is recognized.

Senator Schumer.

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

Senator SCHUMER. Thank you, Mr. Chairman. I want to thank you for holding this hearing and Senator Leahy for requesting that the hearing be held. I have a couple of questions, but before I do I just want to note that yesterday Senator Nelson, of Florida, and I dropped in a comprehensive bill on identity theft and here are some of the things it would do.

It would create an FTC office of identity theft that would help millions of victims of I.D. theft each year get their identities back through an accessible website, a toll-free phone number and consumer service teams. We all know the hundreds of hours people spend trying to get their identities back.

Second, we would regulate data merchants. It would be similar to the regulation we have done in the Banking Committee. I know you testified before them, Madam Chairperson. It would be akin to what we do with credit bureaus. We would make them register with the FTC. We would institute safeguards to prevent fraudulent access by unauthorized parties and require them to develop authentication processes. In other words, we would actually regulate the use of people's information.

We have a tightrope to walk here. On the one hand, in this new society with computers we want information to be available. It helps commerce. On the other hand, when so much information is available, it is part of people's identity and they have some right to be protected. I think our legislation—we have worked long and hard at it—does walk that tightrope in terms of accuracy and in terms of what can be done.

We do a disclosure box so that people will know what has happened with their information. It is similar to the Schumer box

which has been on credit cards for a long time, which I had championed while I was in the House. We require companies to take reasonable steps to protect sensitive information and we have a whole bunch of provisions about Social Security numbers which make it much harder, not impossible, but harder, without justification, to use Social Security numbers.

So this is the basic outline of the legislation, which I think is comprehensive. I think we have had lots of pieces out there from the States, a few here federally. The notification proposal that Senator Feinstein has championed, I think, is excellent and we want to support that as well. But these are things in terms of regulating the companies and things like that.

[The prepared statement of Senator Schumer appears as a submission for the record.]

Senator SCHUMER. So I want to ask you, Chairwoman Majoras, when I talked with you in front of the Senate Banking Committee you were unsure whether the FTC had jurisdiction over data brokers like ChoicePoint and some of the others where we have seen problems. This lack of clear jurisdiction risks leaving data brokers subject to a confusing and incomplete patchwork of laws. In our legislation, Senator Nelson and I give the FTC clear jurisdiction to regulate data merchants like ChoicePoint.

Do you agree that a clear mandate for the FTC would go a long way in clearing up the confusion about the laws and better protect consumers? Do you also agree that it would help stop the situations we have seen with many companies like ChoicePoint and LexisNexis to have clear jurisdiction over these companies?

Ms. MAJORAS. Thank you, Senator. The FTC currently does have jurisdiction, but it is under a patchwork of a couple of different laws. Just to be absolutely clear, I haven't had an opportunity yet, Senator, nor has my staff to review your bill closely.

Senator SCHUMER. We sent it to you.

Ms. MAJORAS. Yes, and we appreciate that. We look forward to reviewing it very carefully and, where we have found any gaps in the law, to work with you on whether this is the right legislation to fill those gaps.

Senator SCHUMER. I would just ask could you respond to us for the Committee record about the legislation in, say, within a week? Could I ask unanimous consent that we get a response within a week, or is that too quick?

Ms. MAJORAS. It is a bit quick because lots of bills are coming in at a rapid rate, and so a couple of—

Senator SCHUMER. Then I will just ask you to get a response to us quickly.

My final question is this: One of the biggest complaints I have heard from constituents on identity theft is people don't know where to go or what to do when their identity has been compromised. When your car breaks down, you know where to go. When you are the victim of a burglary, you know where to go, the local police station. But when you get your identity stolen, you don't know where to go.

What do you think off the top of your head of the idea of creating this office in the FTC of identity theft—we would fund it, obviously;

we would spend $60 million—so that people would have a place to go with experts who could help them clear their names?

Ms. MAJORAS. In my eight months on the job, I don't think I have ever turned down any additional funding, Senator. Thank you. It does sound like perhaps—and, of course, I haven't looked at it, so I have to be cautious.

Senator SCHUMER. Yes, I understand.

Ms. MAJORAS. But it does sound like an expansion of what we are already doing in our office. We have been the clearinghouse for identity theft information and for education and training for consumers, businesses and other law enforcement for years now. We think that message is getting out, which is why we get 15 to 20,000 contacts from consumers a week on identity theft. But by all means, education empowers consumers and we would be happy to expand our education efforts.

Senator SCHUMER. I know my time is about to expire.

Chairman SPECTER. No, no, it has expired.

[Laughter.]

Senator SCHUMER. I would just say the job is not just education, but it is also helping people with their problems, and that is what we would want the office to do.

Ms. MAJORAS. I understand. Thank you.

Senator SCHUMER. Thank you. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Schumer.

Thank you, Chairman Majoras. Thank you, Mr. Swecker. Thank you, Mr. Johnson. Thank you, Attorney General Sorrell. We very much appreciate your testimony and coming in.

The time of the vote has now been deferred until 12:15. You just can't rely on times for votes, but we are still going to maintain meticulous observance of our time limits, and we are going to have a job in getting through the next panel even thus.

If we could now have Mr. Curling, Mr. Sanford, Ms. Barrett, Mr. Dempsey and Mr. Douglas step forward, I would appreciate it.

If you would raise your right hands, do you solemnly swear that the testimony you will present before the Senate Judiciary Committee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. SANFORD. I do.

Mr. CURLING. I do.

Ms. BARRETT. I do.

Mr. DEMPSEY. I do.

Mr. DOUGLAS. I do.

Chairman SPECTER. Let the record show that all five answered in the affirmative.

Our first witness is Mr. Kurt Sanford, President and Chief Executive Officer of U.S. Corporate and Federal Markets for Reed Elsevier's Global Division of LexisNexis Group. He was previously the CEO of LexisNexis Asia-Pacific, a $2 billion division.

We welcome you here, Mr. Sanford, and the floor is yours for five minutes.

STATEMENT OF KURT P. SANFORD, PRESIDENT AND CHIEF EXECUTIVE OFFICER, U.S. CORPORATE AND FEDERAL MARKETS, LEXISNEXIS, MIAMISBURG, OHIO

Mr. SANFORD. Chairman Specter, ranking member Leahy and distinguished members of the Committee, good morning. My name is Kurt Sanford. I am the President and Chief Executive Officer for Corporate and Federal Markets at LexisNexis. I appreciate the opportunity to be here today to discuss the important issues surrounding data security and privacy in the use of commercial data.

LexisNexis is a leading provider of authoritative legal public records and business information. LexisNexis plays a vital role in supporting government, law enforcement and business customers who use our information services for important uses, including detecting and preventing identity theft and fraud, locating suspects, finding missing children, and preventing and investigating criminal and terrorist activities.

LexisNexis works closely with Federal, State and local law enforcement agencies on a variety of criminal investigations. For example, information provided by LexisNexis was recently used to locate and apprehend an individual who threatened a district court judge and his family in Louisiana.

LexisNexis products are also used by financial institutions to help address the growing problem of identity theft and fraud. In 2004, 9.3 million consumers were victimized by identity fraud. Credit card companies report $1 billion in losses each year from credit card fraud. With the use of LexisNexis, a major bank card issuer experienced a 77-percent reduction in the dollar losses due to fraud associated with identity theft. These are just a few examples of some of the important ways in which our products are used by our customers.

While we work hard to provide our customers with effective products, we also recognize the importance of protecting the privacy of the consumer information in our databases. We have privacy policies, practices and procedures in place to protect this information. Our chief privacy officer and privacy policy review board work together to ensure that LexisNexis has strong policies to help safeguard consumer privacy. LexisNexis also has multi-layer security processes and procedures in place to protect our systems and the information contained in our databases.

Maintaining security is not a static process; it requires continuously evaluating and adjusting our security procedures to adjust to the new threats we face everyday. Even with these safeguards, we recently discovered some security incidents at our Seisint business which we acquired last September.

In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. Upon further investigation, we discovered that unauthorized persons using I.D.s and passwords of legitimate Seisint customers may have accessed personal identifying information such as Social Security numbers and drivers' license numbers. No personal financial, credit or medical information was involved, since LexisNexis and Seisint do not collect that type of information.

In March, we notified approximately 30,000 individuals whose personal identifying information may have been unlawfully

accessed. Although no individuals who have responded to our notice have reported any incidents of identity theft or fraud, law enforcement has recently informed us of ten incidents of potential identity fraud where new accounts have been opened. Most of these incidents involve the opening of a new e-mail account or similar activity, while a few involve potential credit card fraud. We are in the process of reaching out to those individuals to put them in touch with the identity theft counselors.

Based on these incidents at Seisint, I ordered an extensive review of data search activity going back to January 2003 at our Seisint unit and across all LexisNexis databases that contain personal identifying information. We have just completed that review and concluded that unauthorized persons, primarily using I.D.s and passwords of legitimate Seisint customers, may have accessed personal identifying information on approximately 280,000 additional individuals. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated, and no customer data was accessed or compromised.

We sincerely regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We will begin notifying those individuals immediately. We are providing all individuals with a consolidated credit report and credit monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity. We also provide them with identity theft insurance to cover expenses associated with restoring their identity and repairing their credit reports.

We are working cooperatively with the U.S. Secret Service and the Electronic Crimes Task Force in their investigation of these crimes. We greatly appreciate the professionalism, specialized skills and efforts provided by the Secret Service and other law enforcement organizations.

We have learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. I have included the details of these enhancements in my written statement.

I note my time is expired. I appreciate the opportunity to be here. In my written statement, I indicated the type of legislation that LexisNexis has already indicated it would support.

[The prepared statement of Mr. Sanford appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Sanford.

We turn now to Mr. Douglas Curling, President and Chief Operating Officer of ChoicePoint. Mr. Curling has had a variety of positions with ChoicePoint, and before was Vice President and Assistant Corporate Controller at Equifax.

We welcome you here, Mr. Curling, and we would be interested to know what your company has found, the breaches, and what you have done about them. The floor is yours for five minutes.

STATEMENT OF DOUGLAS C. CURLING, PRESIDENT AND CHIEF OPERATING OFFICER, CHOICEPOINT, ALPHARETTA, GEORGIA

Mr. CURLING. Chairman Specter, Senator Leahy and members of the Committee, good morning. I am Doug Curling, President and Chief Operating Officer of ChoicePoint. At ChoicePoint, we recognize that in an increasingly risky world, information and technology can be used to help create a safer, more secure society. At the same time, we know, and have been painfully reminded by recent events, that there can be negative consequences to the improper access of personally identifiable information.

On behalf of ChoicePoint, let me again offer our sincere apology to those consumers whose information may have been accessed by criminals who perpetrated this recent fraud. As a result of these experiences, we have made fundamental changes to our business model and products to prevent this from happening in the future.

By way of background, ChoicePoint is a leading provider of identification and credential verification to businesses, governments and non-profit organizations. We have 5,000 associates in 60 locations. We serve more than 7,000 Federal, State and local law enforcement agencies, as well as a significant number of Fortune 500 companies, more than 700 insurance companies and many large financial services institutions.

The majority of transactions our business supports are initiated by consumers. Last year, ChoicePoint helped over 100 million American consumers secure home and auto insurance, more than 7 million American consumers get jobs from our workplace solutions pre-employment screening services, and more than 1 million consumers obtain expedited copies of their vital records—birth, death and marriage certificates.

In addition to helping consumers, ChoicePoint helps agencies at all levels of government fulfill their mission to safeguard our country and its citizens. Our products and services are also used by many non-profit organizations. For example, we have identified 11,000 undisclosed felons among those volunteering or seeking to volunteer with the Nation's leading youth service organizations.

Mr. Chairman, apart from what we do, I also understand that the Committee is interested in how our business is regulated by Federal legislation as well as various State regulations, including the FCRA, the recently enacted companion FACT Act, the Gramm-Leach-Bliley Act and the Drivers' Protection Act.

Sixty percent of ChoicePoint's business is driven by consumer-initiated transactions, most of which are regulated by the FCRA. These include pre-employment screening, auto and home insurance underwriting services, tenant screening services, and facilitating the delivery of vital records to consumers.

Nine percent of ChoicePoint's business is related to marketing services, none of which include the distribution of personally identifiable information. Five percent of ChoicePoint's business is related to supporting law enforcement agencies in pursuit of their investigative missions through information and data services.

Six percent of our business supports law firms, financial institutions and general businesses to help mitigate fraud through data and authentication services. Finally, 20 percent of our business

consists of software and technology services that do not include the distribution of personally identifiable information.

Financial and identity fraud is a rapidly growing and costly threat to our Nation's economy. While we offer a wide range of tools to help avoid fraud, no one is immune to it, as we and other companies and institutions have learned. ChoicePoint has previously provided Congress with information about how identity thieves in California were able to access our products. As you know, California has been the only State that requires consumers to be notified of a potential breach of personally identifiable information.

Contrary to prior statements at this hearing, we not only followed California law, we built upon it and voluntarily notified consumers who may have been impacted across the country, and we did that before anyone called upon us to do so.

We have also taken other steps to help the system protect consumers who may have been harmed in this incident. First, we arranged for a dedicated website and toll-free number. Second, we provided free of charge a three-bureau credit report. And, third, we are providing free of charge a one-year subscription to Credit Monitoring Service.

In addition to helping those affected consumers, we have taken strong remedial action and made fundamental changes to our business and products. First and most importantly, ChoicePoint has decided to discontinue the sale of information products that contain personally identifiable information, unless these products and services meet one of three tests.

First, the product supports consumer-driven transactions such as insurance, employment and tenant screening, or provides consumers with access to their own data. Second, the product provides authentication or fraud prevention tools to large accredited corporate customers where consumers have existing relationships, and, third, when personally identifiable information is needed to assist Federal, State or local government and criminal justice agencies in their important missions.

We have also significantly reviewed and strengthened our credentialing process. We are recredentialing broad sections of our customer base, including more stringent diligence like bank references and site visits. We have created an independent office of credentialing compliance and privacy that reports directly to the board of directors' privacy committee. Finally, we appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the Federal Government's Nigerian organized fraud crime task force, to serve as our liaison to law enforcement.

My testimony includes the legislation we would support and we welcome the opportunity to work with this Committee in trying to address this important issue.

[The prepared statement of Mr. Curling appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Curling.

Our next witness is Ms. Jennifer Barrett, Chief Privacy Officer of Acxiom Corporation. She has been with the company since 1974, after receiving a degree in mathematics and computer science at

the University of Texas. She has had a series of important positions with the company.

We welcome you here today, Ms. Barrett, and look forward to your testimony.

STATEMENT OF JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION, LITTLE ROCK, ARKANSAS

Ms. BARRETT. Thank you, Chairman Specter, Senator Leahy, distinguished members of the Committee. Thank you for allowing Acxiom the opportunity to participate in today's hearing, and I ask that my written statement be inserted into the record.

Chairman SPECTER. Without objection, your full statement will be made a part of the record.

Ms. BARRETT. Thank you.

Mr. Chairman, let me be blunt. The bad guys are smart and they are getting more organized. They are using their skills to illegally and fraudulently access information. Acxiom must therefore remain diligent and innovative by constantly improving, auditing and testing our systems and, yes, even learning from security breaches in the marketplace.

Information is an integral part of the American economy and Acxiom recognizes its responsibility to safeguard the personal information it collects and brings to market. As FTC Chairman Majoras recently stated in testimony before both the Senate and the House, there is no such thing as perfect security and breaches can happen even when a company has taken every reasonable precaution. Although we believe this is true, no one has a greater interest than Acxiom in protecting its information because our very existence depends on it.

Acxiom's U.S. business includes two distinct components—our customized computer services and a line of information products. Our computer services represent more than 80 percent of the company's business and help businesses, not-for-profit organizations, political parties and government manage their own information. Less than 20 percent of Acxiom's business comes from its four information product lines—fraud management products, background screening products, directory products and marketing products. Our fraud management and background screening products are the only Acxiom products containing sensitive information and they represent less than 10 percent of our business.

Acxiom would like to set the record straight in response to a number of misunderstandings that have developed about the company. First, Acxiom does not maintain one database containing dociers on anyone. Instead, we maintain discreet, segregated databases for every product.

Second, Acxiom does not commingle client information from our computer services with our information products. Such activity would constitute a violation of our contracts and consumer privacy.

Third, Acxiom's fraud management products are sold only to a handful of large companies and government agencies who have a legitimate need for them. The information utilized in these products is covered under the safeguard and use rules of the Gramm-Leach-Bliley Act and both State and Federal drivers' privacy protection laws.

Fourth, Acxiom's management verification services only validate information already in our clients' possession. Access to additional information is only available to law enforcement and the internal fraud departments of large financial institutions and insurance companies. Fifth, our background screening products are covered under the Fair Credit Reporting Act. We do not pre-aggregate any of the information for this purpose.

Beyond these protections, the following additional safeguards exist. First, because Acxiom has blended public information with regulated information in both our fraud management and background screening products, we voluntarily apply the more stringent security standards to all such blended data, even though not required by law.

Since 1997, Acxiom has posted a privacy policy on our website describing our on- and offline practices, thus voluntarily subjecting the company to the FTC rules governing unfair and deceptive conduct.

Third, the company has imposed our own more stringent, restrictive guidelines on sensitive information such as Social Security numbers. Fourth, all of Acxiom's products and practices have been audited on an annual basis since 1997 and our security policies are regularly audited both internally and externally by our clients.

Two years ago, Acxiom experienced a security breach on one of our external file transfer servers. Fortunately, the vast majority of the information involved was of a non-sensitive nature and law enforcement was able to apprehend the suspects and ascertain that none of the information was used to commit identity fraud. Since then, Acxiom has put even greater protections in place for the benefit of both consumers and our clients.

In concluding, ongoing privacy concerns indicate that adoption of additional legislation may be appropriate. Acxiom supports efforts to pass federally preemptive legislation requiring notice to consumers in the event of a security breach which places the consumer at risk of identity fraud, and we also support the recent proposal from FTC Chairman Majoras and her comments today extending the GLBA safeguards rule.

Mr. Chairman, on behalf of Acxiom, I want to express our gratitude for the opportunity to participate in this hearing and we are happy to answer any questions the Committee may have.

[The prepared statement of Ms. Barrett appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Ms. Barrett.

We now turn to Mr. James Dempsey, who is the global Internet policy head for the Center for Democracy & Technology. He has a record of having been deputy director for the Center for National Security Studies, special counsel to the National Archives, and with a House Judiciary subcommittee in the past.

Thank you for joining us, Mr. Dempsey, and we look forward to your testimony.

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY, WASHINGTON, D.C.

Mr. DEMPSEY. Good morning, Mr. Chairman, Senator Leahy. Thank you for the opportunity to testify this morning.

We are at a historic moment, I think, today at this hearing for four reasons. First of all, the recent security breaches at a range of companies and institutions have opened a window on the really extraordinary changes that have occurred to the information landscape in recent years.

There is no need to demonize the information service companies. The goal is not to put them out of business. They serve very legitimate purposes, as we have heard today, but they have grown up very rapidly and now it is time for the law to catch up, to provide a framework of oversight and accountability.

Secondly, the debate over harms is now ended. It is clear that the lack of a privacy and security framework is causing real harm to individuals. This isn't some hypothetical debate about marketing data.

Third, the concerns go beyond security and the harms go beyond identity theft. If people are being screened for employment or being denied jobs or screened by landlords and denied the ability to rent an apartment, those are real harms. People should have a right to see that information that is used and the right to challenge it, and the companies compiling it should have some responsibility for its accuracy. The Fair Credit Reporting Act covers many of those applications, but has gaps.

Finally, the industry itself is now open to closing some of the gaps in the law, as you have heard at the table today. So we have an urgent situation. We clearly lack an adequate policy framework. How do we make sure we do not squander this opportunity? There are five sets of policy responses for this Committee and for the Congress.

As a first step toward mitigating identity theft, entities, including universities and government agencies, holding sensitive personal data should be required to notify individuals in the event of a security breach. Since leading information service companies already have spoken in favor of Federal legislation, there is no need to dwell on this other than to say that it makes no sense to enact a law weaker or less comprehensive than the California law. Also, part of the notice solution should be options about what consumers can do when they receive notice. There should be easier ways to freeze credit reports or to put more permanent fraud alerts on credit reports.

Secondly, since notice only kicks in after a breach has occurred, Congress should require entities that electronically store personal information to implement security safeguards similar to those required by a California law AB 1950 and the regulations under Gramm-Leach-Bliley.

Third, Congress should impose tighter controls on the sale, disclosure and use of Social Security numbers. Senator Feinstein has been a leader on this issue for a number of years and the time to address this issue has clearly come. We should take the Social Security number out of the credit header. I don't see any need to send

that out in response to a name query, or to use that in the credit header.

I think we need to shut down the kinds of sales of Social Security numbers illustrated by Mr. Douglas. Keep the Social Security number off student I.D. cards and employee cards and medical insurance cards. Also, we need somehow to break the habit of using the Social Security number as an authenticator. People treat it as if it is a secret or a PIN number, when it is clearly widely available.

The fourth and fifth areas of policy that require addressing concern the legitimate uses of data, because even legitimate uses of data have consequences if the data is inaccurate. Several Senators raised what I consider to be the fourth set of policy issues, which is the Federal Government and other government agencies' use of information brokers. Clearly, national security and law enforcement are legitimate uses, but that doesn't mean we should leave aside questions of accuracy. As a first step, we clearly need to get a handle at least on what information the Federal Government is purchasing and how it is using it.

Finally, Congress needs to look at the fair information practices that have helped define privacy in the credit and financial sectors and adapt them as appropriate to this new data landscape. It is most important here—and I will conclude—to focus on consequences. When data is used in ways that have implications for people's insurance or whether their claims get paid or for a host of other reasons that may not be covered by current law, we need to fill those gaps.

A book was written recently entitled *No Place to Hide*.

Chairman SPECTER. Mr. Dempsey, your time has expired. Would you please summarize?

Mr. DEMPSEY. Is there no place to hide? Senator, really it doesn't have to be that way. We can shape the policy to reclaim our privacy and to set some framework of accountability.

Thank you.

[The prepared statement of Mr. Dempsey appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Dempsey.

We now turn to Mr. Robert Douglas, who has already been introduced and has already testified.

You still have five minutes left, Mr. Douglas.

Mr. DOUGLAS. Thank you. I appreciate that.

As I discussed in the opening presentation and concluded with the murder of Amy Boyer, I would like to concentrate on some of the facts in that case that illuminate, I think, many of the issues that we are discussing here today and what I have learned over the last eight years about information brokers and the harm that can occur.

The facts behind the murder of Amy encapsulate all the issues before this Committee today. Amy's murder demonstrates the problem is much larger than recent breaches of information broker databases.

In October 1999, Amy was entering her car, having just left work. A stalker named Liam Youens pulled alongside Amy and shot and killed her, then killed himself. Youens published his plans to murder Amy on a website for several years, but that website

contained more than the perversity of Youens. It contained a trail of evidence proving personal information gathered with good intent can lead to incalculable harm.

Youens decided to ambush Amy at work, but didn't know where she worked. He used information brokers and private investigators to find her. On the Internet, Youens bought Amy's date of birth, Social Security, home address, and finally place of employment. Youens himself was struck by how easily he could buy Amy's personal information, writing on his website "It is actually obscene what you can find out about a person on the Internet."

The Internet site Youens found was Docusearch.com. Docusearch located Amy's work address by using her Social Security number and other personal information as elements of a deceit designed to fool Amy and/or her mother into revealing the employment address. Indeed, this was Docusearch's expertise. Like many other companies that I demonstrated this morning, at the time of Amy's murder Docusearch specialized in defeating the information security systems of financial institutions, telecommunications companies and unsuspecting citizens with information about loved ones.

But the evidence in Amy's murder doesn't end there. It leads to thousands of documents showing how databases of American businesses that contain our most personal information are breached everyday. As mentioned, Docusearch was penetrating the information systems of financial institutions, telecommunications firms, other utility companies, and selling that information to just about anyone.

In the files of Docusearch and other similar companies is evidence that when it comes to being guardians of personal information, both government and the private sector deserve a failing grade. Several years ago, I worked with the FTC to catch information brokers selling citizens' personal financial information. The investigation revealed hundreds of Internet-based information brokers and private investigators advertising the sale of personal information, in violation of laws Congress has already passed, including Gramm-Leach-Bliley, the FCRA, the DPPA and the Unfair and Deceptive Trade Practices Act.

Many of the illicit information brokers have subscriber access to legitimate information brokers similar to those at the table here at this moment. The illegitimate brokers, along with I.D. thieves, as we have learned, need the biographical information contained in the databases of the legitimate information brokers in order to carry out their crimes.

Specifically, some will purchase the biographical data needed by means of a legitimate information broker via a fraudulent subscriber agreement, as in the ChoicePoint case, or via a reseller who obtains the information from a legitimate broker, then willingly violates the "no resale" clause of their contract. This is the worst-kept secret in the information broker-private investigative world today.

While a number of the major brokers have announced they will restrict access to certain subscriber classes, absent legislation, other companies will step in. But even if all legitimate information brokers were secure, the flow of information would continue. Crimi-

nals and others will just continue to access databases from the government and private sector.

And there is a reason these databases are easily defeated. Far too often, personal biographical information, as we see for sale on the charts in the Committee room today, is the key to unlocking the databases. So even if Social Security numbers were not for sale on the Internet, the reality is Social Security numbers have been compromised in this country in many ways for such a long period that it is laughable that either government or commercial enterprises use the number or other biographical personal information as identifiers for maintaining security of databases.

Yet, this is the method chosen by more than 50 percent of the Nation's banks, telecommunications companies, hospitals, doctors' offices, universities, utility providers, government programs and almost any government or commercial entity one can name. The bottom line: any information security system using personal biographical information as the primary security identifier is fatally flawed.

Thank you.

[The prepared statement of Mr. Douglas appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Douglas.

Mr. Sanford, I am advised that LexisNexis just yesterday announced a breach of security involving some 310,000 people. Did that announcement yesterday have any connection with this hearing scheduled for today?

Mr. SANFORD. The announcement had everything to do with the conclusion of a review that I commenced in February of 2005. As I testified, we acquired the Seisint business in the fall of 2004. One of our integration teams became aware of some irregular billing activities in February.

Chairman SPECTER. That is a no?

Mr. SANFORD. That would be a no, Senator.

Chairman SPECTER. You stated an investigation in February, but you knew about the breach in February?

Mr. SANFORD. We became aware of some irregular billing activities in February.

Chairman SPECTER. Did you know about the breach in February?

Mr. SANFORD. I didn't know what I had until I did an investigation, Senator.

Chairman SPECTER. Well, I am still uncertain as to whether you knew about the breach. Did you have enough information—

Mr. SANFORD. We were not—

Chairman SPECTER. Let me finish the question, since I didn't get an answer to the last one.

Did you know in February that there was a breach?

Mr. SANFORD. I knew in February that I had irregular billing activity in a handful of customer accounts.

Chairman SPECTER. Well, why would it take until mid-April to make a determination sufficient to notify the people whose information had been breached?

Mr. SANFORD. That is an excellent question and I am glad you have asked it because it seems to have been misreported in the press. We are not talking about an incident. In March, we made

a statement acknowledging that we had discovered a handful of security breaches and we immediately made notice.

Based on those incidents, I ordered a review going back some 27 months in our business that we had—

Chairman SPECTER. Mr. Sanford, I don't want to cut you off, but there are five minutes and I have got a lot of questions of this panel. I would like the specifics in writing focusing on why the people whose information was breached couldn't have been notified earlier.

Those people are all at risk and you have a duty to notify them at the earliest possible moment. So I want to know precisely what you did, what was the intensity of your investigation and whether it could have been done faster.

Mr. SANFORD. I would be happy to provide that.

Chairman SPECTER. Mr. Curling, I am advised that ChoicePoint had a breach in the past and did not report it. Is that true.

Mr. CURLING. There has been a recent arrest, or conviction, rather, reported by the Secret Service that involved ChoicePoint information. My understanding is that the subpoena was issued on that individual in 2001.

Chairman SPECTER. Well, see, I am having a hard relating your answer to my question. Did ChoicePoint have a breach of security and failed to report it and notify the people whose information had been breached?

Mr. CURLING. Yes, sir, it would appear in 2001 that happened.

Chairman SPECTER. And it was not reported?

Mr. CURLING. No, it was not reported.

Chairman SPECTER. Why not?

Mr. CURLING. No one was made aware of it, sir. We turned over the information to law enforcement, didn't know the purpose of their investigation.

Chairman SPECTER. No one was made aware of it? Well, how about the person who turned it over to law enforcement?

Mr. CURLING. I don't think that person understood the purpose of the subpoena, sir.

Chairman SPECTER. Well, where did that person stand in the company hierarchy? Somebody who has the authority to turn it over to law enforcement doesn't know enough to say confidential information is now out and it ought to be reported and these people ought to be told about it?

Mr. CURLING. Current circumstances would certainly cause that to happen. Going back four years—

Chairman SPECTER. Well, I am talking about before. Why not?

Mr. CURLING. I can't explain why someone four years ago didn't—

Chairman SPECTER. Well, Mr. Curling and Mr. Sanford, we may well face the necessity for some really tough legislation that will have you do your duty. It is very, very disconcerting that ChoicePoint doesn't make a report of it. A lot of people are at risk and subject to damage.

I would like you also to provide more detailed information as to what you testified, Mr. Sanford, about identity theft insurance—people have to pay for it—whether you have been sued by people whose information has been disclosed.

Let me turn to the Social Security number question, Mr. Dempsey and Mr. Douglas. You need the Social Security number to report your wages and get that information to the Federal Government so they know what your Social Security claim is.

What problem would arise if we legislated that you couldn't use the Social Security number at all, except for purposes relating to collecting Social Security taxes and having the employee get the benefits?

You may both answer. My time is now expired.

Mr. DEMPSEY. Well, that was the original purpose, of course, Senator, and over the years a lot of people became dependent upon the Social Security number as an identifier for purposes unrelated to Social Security. For connecting people, it is not perfect, but it is better than name and address, and that is how people use it.

Now, at the very least we need to begin to wean away from that. I think you would need some kind of implementation time frame to get people that are currently dependent upon the Social Security number for aggregating data and for knowing which Jim Dempsey it is—they use the Social Security number for that. I think we should right away stop using it as an authenticator, which is different from an identifier. People are using it to determine that someone calling up and saying he is Arlen Specter is, in fact, Arlen Specter, when the Social Security number, we know, is widely available.

Chairman SPECTER. There are a lot of people with that name.

[Laughter.]

Mr. DEMPSEY. I can guarantee you that there are probably more than one, Senator.

Chairman SPECTER. I doubt it, but okay.

[Laughter.]

Chairman SPECTER. Senator Leahy.

Senator LEAHY. In the Senate, there is only one.

Mr. DEMPSEY. That is true.

Senator LEAHY. I understand what you mean, Mr. Dempsey. The name is not enough.

Mr. Curling, the CEO of ChoicePoint recently wrote a book about the information industry entitled *The Risk Revolution*. In the book he said everyone should have a right of access to data that is used to make decisions about them, subject to law enforcement and national security exceptions. He also recommended that we expand the principles of the Fair Credit Reporting Act to all types of information—right to access, right to question the accuracy and prompt review, right to comment if a negative record is found to be inaccurate. The Fair Credit Reporting Act also includes procedures to delete inaccurate information and identifying sources that furnish disputed information.

Does ChoicePoint support the expansion of these principles from fair credit to all types of information?

Mr. CURLING. We certainly do, sir.

Senator LEAHY. This past January 20, the Washington Post quoted a ChoicePoint executive as saying, "We do act as an intelligence agency gathering data, applying analytics." He also reported that ChoicePoint acquired I2, Inc., and quoted an I2 company executive as saying, quote, "We are principally a company

whose focus is all about converting large volumes of information into actionable intelligence," close quote.

The article described I2 as a company that uses software to head off crimes or attacks, not just investigate them after the fact—sort of something like the movie "Minority Report." How would you head off a crime? How do you identify a potential crime or criminal? Do you have predictive algorithms or profiling, risk-scoring? It seems fascinating as a former prosecutor. Can you just put us all out of business? Can you tell who is going to commit a crime?

Mr. CURLING. These are tools that ChoicePoint sells to law enforcement agencies. They are the ones that use the tools to try and figure out how to solve crimes, and largely the data they are using is data they gather on their own. I2 is a software company. It is a company that provides a robust analytic engine to link disparate data together so you can look for similarities.

If two people don't necessarily know each other but they both made phone calls to the same phone number, you can look for that kind of linkage through vast amounts of data. They use it as an analyst aid for an analyst to almost interact with the data iteratively and reach conclusions that they might otherwise have reached doing manual research, but in a much faster way.

Senator LEAHY. To identify a crime before it happens?

Mr. CURLING. Or just look at patterns to try and track down criminals that have suspicious behavior going on.

Senator LEAHY. ChoicePoint also purchased—is it Bode Technology?

Mr. CURLING. Yes, sir.

Senator LEAHY. A company that specializes in the use of DNA to identify people. The CEO, Derek Smith, wrote in his book, "Biometrics provide an opportunity to shore up the society's fundamental building blocks of identification through technology."

Biometrics is a technology with great potential, but there are concerns. Unlike a Social Security number which actually is changeable, with some difficulty, but can be changed, a fingerprint or other biometric compromised by a security breach can't be replaced. There are technological limitations. We found that with facial recognition technology that that doesn't always work.

What types and how much biometric information, if any, is contained or accessible in the systems at ChoicePoint or any of its subsidiaries, and under what conditions is it used or provided and what are the protections?

Mr. CURLING. We don't warehouse biometric data. We don't maintain biometric databases on behalf of anyone. Bode Labs is a forensic DNA laboratory that supports law enforcement activities on an outsource basis. That laboratory was the lab that identified the victims of the World Trade Center from a DNA perspective. That laboratory had a scientist over in Thailand recently for the tsunami aid.

It is a law enforcement outsource laboratory that does very high-technology DNA assistance in prosecution of cases. They receive samples directly from law enforcement. They manage the chain of custody of that sample and they turn it back over to law enforcement when the lab activities are processed.

Senator LEAHY. Thank you.

Mr. Dempsey, government relies more and more on the services and products of data brokers for law enforcement and homeland security efforts. Is this allowing the government to access and use information that otherwise it might not be allowed to under privacy and information laws? In other words, does it allow them to do a search that they wouldn't be allowed to do if they were doing it directly through a government agency?

Mr. DEMPSEY. Well, it does allow them to, in essence, outsource data collection activities outside of the Privacy Act. Right now, if the government is going to start a new collection of data, it needs to comply with the Privacy Act and it needs to perform a privacy impact assessment. But if it goes and buys that same data or subscribes to it, some of those rules don't apply, and I think that is an issue that needs to be definitely included in the scope of these hearings and needs to be addressed in legislation.

Senator LEAHY. Thank you. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Leahy.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much.

The California law went into effect in 2003. I would like to ask each of the people here representing companies to indicate if, prior to 2003, you had a breach and did not notify people.

Mr. Sanford?

Mr. SANFORD. I believe there were security breaches in the business that I acquired that I mentioned, Seisint. I believe there may have been a security breach in LexisNexis prior to 2003, and we did not make notice prior.

Senator FEINSTEIN. Thank you. I appreciate the honesty.

Mr. Curling?

Mr. CURLING. Yes, ma'am, I previously indicated there was a breach that we didn't notify them.

Senator FEINSTEIN. Thank you.

Ms. Barrett?

Ms. BARRETT. The breach that we had in 2003 did span the enactment of the law in July. Our obligation as a provider, since the breach did not involve—

Senator FEINSTEIN. My question is did you have a breach prior to the 2003 law going into effect?

Ms. BARRETT. Yes, the breach that we had did span it, but we did provide notice to our clients.

Senator FEINSTEIN. Thank you. This is my point: If it weren't for the California law, we would have no way of knowing breaches that have occurred. It is really only because of that law that we now know. We in no way, shape or form are able to pierce the depth of what has happened in this industry.

Now, I would like to ask the question of each, how did the data breach or breaches occur and what has been done to correct it? Who would like to go first?

Mr. Sanford?

Mr. SANFORD. The data breaches that we have reported principally involve compromised passwords and I.D.s of legitimate customers, and that happened through a variety of methods.

Senator FEINSTEIN. Could you explain "compromised?"

Mr. SANFORD. Sure. Where a company has individual users, each person would have an I.D. and would have a password. A company may report to us that they notice search activity that showed up on their bill that they said that they didn't do.

Senator FEINSTEIN. Now, take a big company. How many people would have a password?

Mr. SANFORD. In most companies, there would be individual I.D.s and individual passwords. There were some instances in—

Senator FEINSTEIN. But how many per company?

Mr. SANFORD. It depends, Senator. You could have two. You could have 10,000.

Senator FEINSTEIN. That is correct, so that a large bank like a Citibank could have a large number of individuals that would have passwords to the system, correct?

Mr. SANFORD. I.D.s and passwords, that is correct.

Senator FEINSTEIN. I am asking for speculation. I don't know what they have, but this is a weak link, shall we say.

Mr. SANFORD. Well, passwords and I.D.s are part of the security and when those password and I.D. protocols are not strong, then you do have a weak link in the system. What we have found is we have weak links in some of the passwords and I.D.s in some of our customer environments that were compromised and unauthorized persons gained access to those passwords and I.D.s and did searches.

Sometimes that was because it was a weak password-I.D. combination. Sometimes that was because there may have been virus in that business and someone compromised it through criminal means.

Senator FEINSTEIN. Right, and did you find out who that person was?

Mr. SANFORD. We have referred all of these incidents to the U.S. Secret Service and it is an ongoing investigation.

Senator FEINSTEIN. Were those persons found out?

Mr. SANFORD. I don't know. That is not the kind of information they share with me.

Senator FEINSTEIN. And you didn't think you would be interested in finding out?

Mr. SANFORD. Well, as the agent in charge advised me, he will be briefing us on it as they conclude their investigation.

Senator FEINSTEIN. You have had more than one breach, though.

Mr. SANFORD. That is correct.

Senator FEINSTEIN. So there are a number of people whose passwords have been compromised.

Mr. SANFORD. That is correct.

Senator FEINSTEIN. Which means they could have sold them for a lot of money to somebody else who got into the system.

Mr. SANFORD. That is a possibility, so each password and I.D.—

Senator FEINSTEIN. But you have no knowledge. How many breaches have you had?

Mr. SANFORD. We reported 59 incidents going back to the beginning of 2003.

Senator FEINSTEIN. And these were all from compromised passwords?

Mr. SANFORD. I believe all but four or five of them were through compromised password I.D.s.

Senator FEINSTEIN. And you don't know who compromised the passwords?

Mr. SANFORD. I don't know who did.

Senator FEINSTEIN. Okay, that is fine.

I want to go down the line on this and then back on what you have done. Mr. Curling, how many breaches have you had, total?

Mr. CURLING. The breaches that we investigated and reported were a number between 45 and 50. It was an organized ring of fraudsters and they hijacked legitimate business identities or created false business identities and were able to get through our credentialing processes. We ultimately identified that activity when they were trying to set up accounts, but unfortunately and regrettably, accounts had been set up prior to that.

Senator FEINSTEIN. Ms. Barrett?

Ms. BARRETT. Yes. The breaches that we had in 2003 involved two different individuals.

Senator FEINSTEIN. How many breaches have you had, total—has Acxiom had?

Ms. BARRETT. These are the only two breaches.

Senator FEINSTEIN. You have only had two breaches, okay.

Ms. BARRETT. They involved a file transfer server sitting outside of our main system that was used to send information back and forth between our clients. They did not penetrate our main firewalls of the system. The data on this server belonged to our clients. The data was breached because an individual at a client location with legitimate access to that server downloaded the password file for that server and unencrypted a portion of the encrypted passwords, then used those passwords to access other people's data.

Senator FEINSTEIN. My time is up. Can I ask just one other question? I have sat here patiently all morning.

Chairman SPECTER. Yes, you may, Senator Feinstein.

Senator FEINSTEIN. Just one other question and this is on the subject of whether there should be a requirement that all data in these data companies be encrypted and there should be a prohibition on using PCs to hold this data. I am looking specifically at University of California data breaches which involved the names of over 700,000 people from thefts of personal computers.

Would anyone care to comment on that?

Mr. DEMPSEY. Senator, I would only say that encryption is not as easy to do as it sounds and I would hate to see the Federal Government get into the posture of dictating specific security measures that companies or institutions like universities have to take.

Senator FEINSTEIN. So you think it is okay for personal data, for somebody to be walking around with a computer with 700,000 names in it?

Mr. DEMPSEY. Well, I think there is a separate question about the physical custody of that kind of—at some level, that is a physical custody issue. If you look at the Gramm-Leach-Bliley regulations, they talk about technical, physical and administrative safeguards. And I think without, again, dictating what is the right balance of those, all three have to be considered. And I agree with you that people have clearly gotten far too lax about storage of data.

Senator FEINSTEIN. Thank you. My time is up.

Chairman SPECTER. Thank you, Senator Feinstein.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman, and I have a question I am going to ask of the whole panel, but take your pencils out because it has a few parts. I want to ask your opinion on various ways to deal with identity theft, all of which are embodied in the legislation that we have. If you could give us a yes or no answer, that would be great and save time. If you can't, keep your explanation as short as possible.

Do you support the goal of regulating data merchants, similar to the way we regulate credit bureaus I would say, but certainly data merchants? Do you support the idea of creating a one-stop shop to help consumers get their identity back, as we have done in the FTC? They have done something, but they are not close to what is needed.

Do you support disclosure laws for companies that plan to sell your information? Do you support making any company that has sensitive personal information on its consumers take reasonable steps to protect it? That would be the words of the law—"reasonable steps to protect it." Do you support limiting the sale of people's Social Security numbers on a narrow needs basis—law enforcement and things like that?

Just two more. Would you support rules authenticating customers? This relates to ChoicePoint, which actually sold the information to criminals. And would you support increased background examination of those within your companies and other companies who have access to sensitive personal information?

I realize that is a long question. It will be my only one and I await your answers.

Mr. Sanford?

Mr. SANFORD. Senator, I don't know if I got it all down, but I think the first one was with respect to regulating the industry similar to FCRA. I think some of the portions of the FCRA could be appropriate. I would like to see specifically what the wording would be on that. I would be glad to work with you on that.

A one-stop shop at the FTC.

Senator SCHUMER. But, in general, you support regulating data companies like yours in terms of how they deal with the data, data merchants?

Mr. SANFORD. I certainly think the safeguards as contained in GLBA would certainly be a step in the right direction.

Senator SCHUMER. Thank you.

Mr. SANFORD. I don't know anybody who could argue with a one-stop shop at the FTC and additional funding to help, given the pervasiveness of identity theft. I am not sure I understand the provision on disclosure laws on companies. I didn't quite get the rest of it down here in my notes.

We would support data safeguards. We would support legislation—

Senator SCHUMER. That is disclosure to the individual, whoever gives it in, that we may be giving or selling that information to somebody.

Mr. SANFORD. I don't know, unless I saw the wording, whether I could support that, given the number of transactions we are talking about.

Senator SCHUMER. Okay.

Mr. SANFORD. Limiting the sale of SSNs. Certainly, there are limits today on the use of personally sensitive information and I support the limits that are there. I think there could be greater limits on the display of information, but perhaps not the access because of the importance of using some of that sensitive information to provide services to detect fraud, for example.

And then on rules authenticating customers, I think I would support, again, GLBA, and I think reasonable safeguards would pretty much pick that up and say you have got to make sure you are doing business with legitimate customers.

Senator SCHUMER. And then the last one was background checks on the people who handle the sensitive information.

Mr. SANFORD. I would have to learn more about that, but again I think that would be part of an overall safeguard program and make sure that the people who are dealing with sensitive data—

Senator SCHUMER. Thank you.

Mr. Curling?

Mr. CURLING. In the interest of time, Senator, obviously I would like to read the specific proposals, but I would answer yes, in general, to all of the questions.

Senator SCHUMER. Thank you.

Ms. Barrett?

Ms. BARRETT. Yes, I would also say yes, in general, to all of the questions. Many of what you are suggesting are already policies of ours.

Senator SCHUMER. Mr. Dempsey?

Mr. DEMPSEY. I have never seen a vote count like this, Senator. I am a "yes" on all as well.

Senator SCHUMER. And Mr. Douglas?

Mr. DOUGLAS. Absolutely.

Senator SCHUMER. Mr. Chairman, I yield back my 32 remaining seconds.

Chairman SPECTER. It is greatly appreciated, Senator Schumer.

Senator SCHUMER. I knew it would be.

Chairman SPECTER. You now owe the yield-back bank only 17 hours and 23 seconds.

Senator SCHUMER. No good deed goes unpunished.

Chairman SPECTER. On behalf of Senator DeWine, I am going to direct this question to you, Mr. Sanford. Senator DeWine could not be here. I understand that LexisNexis has been working with the National Center for Missing and Exploited Children and law enforcement to help find abducted children. Can you explain to the Committee how LexisNexis contributes to this effort?

Mr. SANFORD. Senator, the National Center, as you know, has been in existence for nearly 20 years. It provides critical assistance to find abducted and missing children. I think in the last 20 years, they have recovered 85,000 children.

What the National Center does is we provide our service to them at no charge. They work with law enforcement and what they have determined is the best way to find an abducted child in the first

48 hours is to do searches and to find the relationships of the custodial and non-custodial parents. And by doing those searches with law enforcement, they are able to recover many of the abducted and missing children rapidly.

Chairman SPECTER. Well, thank you very much, Mr. Sanford, Mr. Curling, Ms. Barrett, Mr. Dempsey and Mr. Douglas.

Senator LEAHY. Could I ask one more question?

Chairman SPECTER. Sure, Senator Leahy.

Senator LEAHY. Mr. Dempsey, you and I have had discussions over the years on some of these issues and I have appreciated very much your input. I think about public records, and let's just take one example. You have whatever court handles divorce matters in your State and you may have divorce records in there which contain a number of things because of payments—Social Security numbers and maybe even the names of the banks that the litigants have, and so on.

If you were to walk into that court and ask, they would say, well, we can give you the judge's findings, the pleadings, of course, but we can't give you this page that has all the rest. So you kind of felt you were pretty safe because had to go to court, to court, to court, to court and be turned down.

Now, if it is all electronic, you don't have that inconvenience. Is there a responsibility on the part of data brokers who might go through every single court in the Nation pulling up *Jones* v. *Jones* or whatever—do they have a responsibility in weeding out the things that the courts would normally expect not to be shown?

Mr. DEMPSEY. Well, I think, Senator, you are on to a very important point, which is just because information is in a public record, does it mean that there are no privacy issues, particularly in terms of accuracy, particularly in terms of sensitivity?

The Supreme Court held in the Reporter's Committee case and in the DPPA case, the *Reno* v. *Condon case*, that even if information is publicly available, interests in accuracy apply, and the computerized compilation of that data into a single database changes the privacy equation. So you can't just say, oh, it is public record information, therefore there are no concerns.

There are still concerns about the accuracy in the transcription of that data and still concerns about the fact that, as you say, in bankruptcy court there is a lot of very sensitive information. I know that bankruptcy judges are struggling with that specifically.

Senator LEAHY. Adoption courts; probate courts handle adoptions. Courts have allegations that are made in initial filings in a case, but the case may be heard six months later and all the allegations thrown out.

Mr. DEMPSEY. So I think that that has to absolutely be part of the equation here. Under the Fair Credit Reporting Act, we have created this cycle of responsibility where the data furnishers have a responsibility for accuracy, the data aggregators and the credit reporting agencies have a responsibility, and the users have a responsibility in terms of accuracy.

It is a little bit different in the public record system, in that the government entities are not pushing that data. It is being pulled by sending people out, but we still have to somehow address that, Senator, and work on what is the responsibility for accuracy of the

compilier of that so-called public record information because it is being used against people in ways that have implications.

Senator LEAHY. And some of it is there for a very, very specific purpose. I mean, you could actually have on public record what kind of alarm systems you have in your house from an appraisal that had been done of the house.

Mr. DEMPSEY. Well, for example, criminal history records. There is a very important public policy interest in having arrests be public, in having court proceedings be public. But we also know that a lot of arrests don't result in convictions for the charges. We have put limits in the fair credit reporting area on reporting of old arrests reporting of so-called naked arrests. I think we need to make sure that those kinds of accuracy responsibilities spread across the data landscape.

Senator LEAHY. Thank you. Thank you, Mr. Chairman. I appreciate again your holding this hearing. I think it is extremely important and I am glad to see the Committee doing this kind of oversight.

Chairman SPECTER. Well, thank you, Senator Leahy. You were the first one on the Committee to ask for it and I promptly responded and said yes. I think it has been a very, very productive hearing and I believe that there will be some very firm Federal legislation coming out of this issue.

Thank you all very much.

[Whereupon, at 12:00 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

[Additional material is being retained in the Committee files.]

QUESTIONS AND ANSWERS

Responses to Written Questions of Senator Patrick Leahy
For Submission in the Hearing of
"Securing Personal Data: Striking a Balance Between
Privacy and Commercial and Governmental Use"

Before the Senate Committee on the Judiciary
April 13, 2005

Responses of Jennifer T. Barrett, Chief Privacy Officer, Acxiom Corporation

Question 1: **Press reports have referenced recent security breaches at Acxiom. Please identify any and all security breaches of Acxiom's systems or databases occurring on January 1, 2002, or later that resulted in unauthorized access to an individual's personally identifiable information. For each incident, please indicate whether the affected individuals received notice of those breaches, and any changes Acxiom implemented in its policies, procedures or systems as a result of those breaches.**

Response: Acxiom has been the victim of two incidents of unauthorized access to consumer data. Those occurred in late 2002 and early 2003. Though the incidents were apparently not related, both involved the same undetected vulnerability in a file transfer server. The files accessed were files belonging to various Acxiom clients while those files were in transit between each of those clients and Acxiom. As a result, Acxiom reported to each impacted client exactly which of their files were potentially accessed. This was done based on a thorough review of the logs of files transferred across the File Transfer Protocol (FTP) Server the perpetrators had access to.

The nature of those logs allowed Acxiom to identify the potentially accessed files by filename, but did not provide the details of what consumers were on each file. As a result, Acxiom was not, and is not, in a position to determine the number of individual consumers whose information may have been accessed. That determination was made by each impacted client after review of the files Acxiom identified to them.

The type of information involved varied greatly among the files. Most files transferred via that server did not contain sensitive information (e.g., SSN, Acct. #, DL #), but were merely statistical reports of processing performed or marketing lists of names and addresses resulting from Acxiom processing services. In the rare cases where files did contain sensitive information, that information was typically truncated or encrypted.

Acxiom quickly addressed the specific vulnerability once it was discovered. In addition, substantial changes were made in the file transfer hardware and software, processes and procedures and policies. Acxiom retained third-party consultants to review and test not only those items, but all aspects of its information security program. Auditing, testing and revision of the information security measures continues on an on-going basis.

Question 2: **What is Acxiom's current policy with respect to allowing individuals to see the information that Acxiom has on them in its systems and distributed databases, including any costs or conditions of access? Do individuals have a right to see *all* of the information maintained on them by Acxiom? If not, please explain.**

Response: Acxiom maintains a Consumer Care Department led by a Consumer Advocate whose team interacted with more than 50,000 consumers in the past 12 months by way of answering questions, resolving issues, processing opt-outs, and handling requests for access to Acxiom's fraud management, background screening, directory and marketing products. Acxiom provides consumers who contact the company (through the company website, or by calling a toll-free Consumer Hotline or by writing to the company) the options of: opting-out of all of Acxiom's marketing products; receiving an information report from the company's fraud management and directory products; or receiving a consumer report as specified in the FCRA from the company's background screening products. Acxiom encourages consumers to notify the company if the information in any of these reports is inaccurate and it is the company's policy either to correct the information, to delete it or to refer the consumer to the appropriate source to obtain the requested correction, such as a county or state agency. The consumer is charged $5.00 for the report concerning the fraud management and directory products. Acxiom does not currently charge a fee for access to the FCRA regulated background screening products.

Given the non-sensitive nature of the marketing products, and Acxiom's prohibition on the use of those products for reference or investigatory purposes, consumers are not provided the ability to see the actual information contained in those products. Consumers who inquire are informed about the types of information in those products and given the opportunity to opt-out of those products.

Question 3: **Recently, during a March 3, 2005 California senate hearing, Don McGuffey, a Vice President at ChoicePoint, testified that "in our new era, we are working today to provide a single point of contact to be able to deliver to consumers who request it, free of charge, a report that would include the variety of products and services that we have delivered and delivered today,...As we can get built a single point of access, a consumer will be able to see the products that they have available to them, request the products at no charge, and we will deliver them."**

Does Acxiom currently have such a single point of contact to allow individuals to access any personally identifiable information that Acxiom provides on them to its customers? If not, will Acxiom join ChoicePoint in committing to create such a single point of contact? If Acxiom will not make such a commitment, please explain why not.

Response: See the response to question 2 above. Acxiom's Consumer Care Department provides the single point of contact for consumers concerning all but one of Acxiom's information products. The FCRA-regulated employment screening operation is completely segregated from Acxiom's other operations and has FCRA-specific procedures for handling consumer inquiries. As a result, the consumer care for that operation is handled separately, but the consumer care advocates assist consumers with contacting both consumer care departments.

Question 4: **On April 20, 2005, *Wired News* reported an announcement by Rapsheets – a division of ChoicePoint, that, whenever one of its customers runs an individual background search on its database for employment or volunteer screening purposes, Rapsheets will notify the individual and provide him or her with a copy of the background report and the name and address of the organization conducting the search, if that search reveals a criminal record. Does Acxiom currently have a similar policy? If not, will Acxiom provide individuals such information in the future? If so, when, and if not, why not?**

Response: Acxiom delivers employment and volunteer screening reports pursuant to the Fair Credit Reporting Act (FCRA). Therefore, the reports are only prepared when authorized by the consumer seeking the position as evidenced by a written application signed by the consumer. In the event an adverse action is taken against that consumer, the employer or organization is required to advise the consumer of their right to receive a copy of the information relied upon and dispute any inaccuracies. Acxiom does not currently advise consumers directly of reported information, but does provide consumers with a copy of the information provided about them, free of charge, if they contact us following an adverse action. Given this longstanding statutory method of making consumers aware of adverse actions and reported criminal records, Acxiom does not believe the policy announced by Rapsheets is necessary.

Douglas C. Curling, President, ChoicePoint Inc. ("ChoicePoint" or the "Company"), hereby responds to the written questions propounded by Chairman Specter in connection with the Senate Judiciary's April 13, 2005, hearing on "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use." I believe the information included in the responses which follow is accurate and represents my best efforts to provide complete responses. I reserve the right to supplement or modify these answers as may be appropriate in light of information, through review of additional documents or otherwise, which may hereafter come to the my attention.

1. **In your testimony, you identified at least one breach regarding which ChoicePoint did not notify affected customers.**

   a. **Please identify and describe all significant, known breaches that ChoicePoint has experienced since January 2001.**

   b. **What gaps in your security allowed these breaches to occur?**

   c. **With regard to each of these breaches, were any of the affected consumers notified? Was law enforcement notified?**

   d. **Prior to the recent revelations regarding breaches at ChoicePoint and other companies, what steps did ChoicePoint take when it discovered a breach involving personal information?**

   e. **Please explain what ChoicePoint is doing about these breaches. What will it do to prevent future breaches?**

The Federal Trade Commission (FTC) is conducting an 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 the 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 those accounts have been notified. Additionally, we found an account recently that we have investigated and identified approximately 100 potentially affected consumers whom we have now notified.

ChoicePoint continues to investigate and work with law enforcement regarding the Los Angeles incident, terminating accounts and/or user names and passwords as appropriate. It should be noted that from time to time ChoicePoint receives requests for information from law enforcement – primarily in the form of subpoenas. Historically, our relationship with law enforcement has been a one-way street whereby we respond as

quickly as possible with the information requested. Many times we do not gain additional information from law enforcement regarding such requests.

ChoicePoint recognizes the importance of securing sensitive data and our security processes always continue to evolve. With respect to consumers affected by the consumer fraud-based security breach that gave rise to the notifications in February and March 2005, ChoicePoint has taken a number of steps in addition to such notifications:

- First, ChoicePoint has established a dedicated toll-free customer service number and a special web site to respond to inquiries;
- Second, ChoicePoint is providing, free of charge, a combined three-bureau credit report;
- Third, ChoicePoint is 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.

In addition, ChoicePoint has strengthened its customer credentialing process and is changing its products and services to many customer segments. It is requiring additional due diligence such as banking references and site visits to customers receiving personally identifiable information before allowing access to personally identifiable information. It is recredentialing sections of its customer base.

ChoicePoint is modifying the services that the company is delivering to its customers. ChoicePoint is also undertaking internal reviews with respect to certain products to examine information security, computer operations and other controls.

ChoicePoint has created an office of Credentialing, Compliance and Privacy that will report to the Board of Directors' Privacy Committee and be independent of ChoicePoint management. This office is led by Carol DiBattiste, previously Deputy Administrator of the Transportation Security Administration, Department of Homeland Security; former Director of the Executive Office for United States Attorneys, Department of Justice; former Principal Deputy General Counsel, Department of the Navy; former Director of the Office of Legal Education, Department of Justice; and former Assistant U.S. Attorney in Southern District of Florida with extensive experience in criminal prosecutions and compliance.

ChoicePoint has 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 liaison to law enforcement officials.

In addition, ChoicePoint has decided to exit the consumer sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will sell information products containing personally identifiable information consisting of date of birth and Social Security and drivers' license numbers only to industries 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 continues to review its responses to the consumer fraud-based security breaches that gave rise to the consumer notifications in February and March 2005, and will continue to take additional steps, as appropriate.

2. Have any affected consumers ever sued ChoicePoint for damages they suffered as a result of a breach? If so, please describe the substance of each suit and its outcome or current status.

Four (4) class action complaints (naming seven (7) plaintiffs) have been filed against ChoicePoint by consumers for alleged damages suffered as a result of the consumer fraud-based security breach that gave rise to the notices sent to approximately 146,500 consumers in February and March 2005. These matters, which are currently pending, are styled as follows:

- *Harrington v. ChoicePoint Inc.* (CV05 1294) (Named plaintiffs: Jennifer Harrington, Jessica Seymour);
- *Salladay v. ChoicePoint Inc.* (CV05 1683) (Named plaintiffs: Travis Salladay, Evelyn O'Keefe, Charles Slavin);
- *Goldberg v. ChoicePoint Inc.* (CV05 2016) (Named plaintiff: Eileen Goldberg); and
- *Cloy v. ChoicePoint Inc.* (CV05 1993) (Named plaintiff: Johnny Cloy)

The above complaints were recently consolidated in the United States District Court for the Central District of California before Judge Mariana R. Pfaelzer. Plaintiffs must file a Consolidated Amended Complaint by June 30, 2005. ChoicePoint's response is due August 1, 2005.

ChoicePoint was served on June 20, 2005, with a consumer complaint, styled *Wilson, et al. v. ChoicePoint Inc.*(1:05 –CV-1604) in the U.S. District Court for the Northern District of Georgia, for alleged damages suffered as a result of the consumer fraud-based security breach that gave rise to the notices sent to approximately 146,500 consumers in February and March 2005. The plaintiffs are William Wilson, residing in

Palm City, Florida; Paul Pagliaro, residing in Staten Island, New York; and Linda Johns, residing in Idaho Falls, Idaho.

3. What is the universe of personal data contained in ChoicePoint's databases? What are the specific sources of this data?

ChoicePoint acquires and maintains data on individuals, businesses, and their assets. Data is obtained from a wide variety of sources, some of which is maintained by ChoicePoint, and some of which is accessed on demand.

The information our company maintains or accesses on individuals is typically obtained from government sources or other information providers. The information source typically falls into one of three categories: non-public, public records or publicly-available. Publicly available information is typically white page phone records. Moreover, we maintain public records such as certain civil record data including bankruptcy, liens, judgments and evictions - information obtained from various state and federal court locations. We also maintain criminal conviction data from certain but not all federal, state and local jurisdictions. Lastly, we also maintain professional licensing and permit information (physicians, pharmacists, attorneys, concealed weapons permits) from state secretaries of state or other various licensing bureaus.

Non-public information sources include credit bureaus that provide certain consumer reports or state agencies that provide drivers license data. Consumer reports are provided in compliance with the Fair Credit Reporting Act (FCRA) and driver's license data is provided in compliance with the DPPA. Likewise, we obtain and provide to our credentialed customers, credit header information (which includes a person's name, address, former address, and Social Security number) consistent with the Gramm-Leach-Bliley Act.

The company maintains data on property (current and prior tax and deed information) and vehicle identification information (automobiles, boats, planes).

ChoicePoint maintains the following types of data on businesses: yellow pages information, business bankruptcies, liens, judgments, pending litigation, Uniform Commercial Code filings, corporate records and business reports. This information typically comes from yellow pages, court records and secretary of state filings.

ChoicePoint does not have banking records, credit card transaction data or medical records. As I discussed during the hearing, our subsidiary Bode Technologies, which processes DNA evidence for law enforcement agencies, does not database any DNA information for reuse in our products or services.

4. In your testimony, you stated that over 60 percent of ChoicePoint's business is covered by FCRA.

a. Please identify specifically which types of personal data collected, held or sold by ChoicePoint, or transactions offered by ChoicePoint, are regulated by FCRA?

ChoicePoint companies offer a range of FCRA-regulated products. These products primarily support transactions involving insurance underwriting, pre-employment screening, tenant screening, and pre-screening for firm offers of credit and insurance. ChoicePoint companies also provide consumer reports pursuant to other FCRA permissible purposes, such as pursuant to the written instructions of the consumer to whom the report relates.

Depending on the nature of the report and the purpose for which the report is provided, consumer reports provided by ChoicePoint companies might include personal identifiers (such as name, address, date of birth, social security number, etc), some of which may be redacted in certain reports. Consumer reports provided by ChoicePoint, again depending on the purpose for which the report may be provided and the particular product offered, may include other data including information such as: insurance claims data; motor vehicle record information; employment history information; criminal history record information; bankruptcy, liens, and judgment information; other civil court information; licensing and sanctions information; eviction data; and demographic data. In addition, ChoicePoint companies may act as resellers of credit reports obtained from one or more of the three nationwide credit bureaus.

b. Please identify which provisions of FCRA apply to each type of data or transaction?

The Fair Credit Reporting Act regulates consumer reports and certain practices of consumer reporting agencies largely without distinction on the basis of particular data types or transactions. There are exceptions to this general rule, however. Section 613 of the FCRA (discussed separately in connection with Question 4.d. below), for example, only applies with respect to the reporting of public record information likely to have an adverse impact on an individual's employment prospects in a consumer report provided for employment purposes. Similarly, FCRA section 604(b) provides additional protections for consumer reports that are provided for employment purposes.

c. Of the personal data that ChoicePoint collects, maintains or sells, and the transactions offered by ChoicePoint, which are not regulated by FCRA?

ChoicePoint companies offer a range of products which are not regulated by the FCRA. ChoicePoint Public Records Inc., for example, provides public record information (such as court records, licensing records, and UCC filings) and publicly available information (such as telephone directory information) for non-FCRA purposes.

Our Insurance Services Division makes public record information and other information available to insurers to assist them in their conduct of insurance claims investigations and processing. In addition, ChoicePoint Precision Marketing Inc., offers a number of marketing-related products and services which are non FCRA-regulated.

Other ChoicePoint companies may also collect or maintain personal information about consumers in the context of non-FCRA-regulated transactions or businesses. Our WorkPlace Solutions unit, for example, facilitates drug testing of employees by their current or prospective employers.

d. FCRA requires that you always notify individuals when you report adverse information about them on an employment check. Do you always do this?

Section 613 of the Fair Credit Reporting Act requires, with a limited exception for national security investigations, that a consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment to either:

> (1) notify the consumer, at the time such public record information is reported to the user of such report, of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or
>
> (2) maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date.

Which of these two options ChoicePoint companies utilize when providing consumer reports for employment purposes containing public record information likely to have an adverse effects upon a consumer's ability to obtain employment varies depending upon the nature of the report being provided. Consumer notice is typically provided in the case of reports generated from databases maintained by ChoicePoint companies, while strict procedures to ensure that public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is complete and up to date typically are utilized for reports where the public record information is collected directly from a public record repository at the time the report is prepared.

5. How do you ensure that the data you collect, maintain and sell is accurate? How accurate do you think the data is?

Last year, we delivered more than 100 million FCRA products - of which less than one-tenth of one percent were disputed by consumers. ChoicePoint takes a number of active measures to ensure the accuracy of data. As a threshold matter, ChoicePoint obtains personally identifiable information only from reputable sources, such as public filings, federal, state, and other governmental authorities, other information companies, and online search systems.

ChoicePoint undertakes regular audits and other internal procedures and safeguards intended to assure the integrity and quality of the personal information that ChoicePoint collects, maintains, or communicates. These procedures include both automated analytics and manual reviews of data both prior to and after its acquisition. While these processes can identify certain anomalies, ChoicePoint is incapable of determining the accuracy of certain information contained in public filings, *e.g.,* whether a publicly recorded lien is in fact valid.

ChoicePoint provides consumers with a right to review data and to correct inaccuracies. To the extent inaccurate information is recorded in public filings, ChoicePoint will direct the consumer to the original source of the inaccurate data so that it maybe corrected at its source. The corrected information would then be reflected in subsequent ChoicePoint reports.

Our non-FCRA public record search products function much like common internet search engines such as Google. Accordingly, the search results returned vary based on the depth and completeness of the search criteria entered, as well as the data available at the time of search.

6. What language would you recommend Congress adopt requiring companies like yours to give notice when they experience a breach?

We believe that giving increased oversight authority to the Federal Trade Commission (FTC) would provide consumers the assurance they deserve. We would further support extending the principles of the Fair Credit Reporting Act (FCRA) to cover all sensitive personally identifiable data regardless of its source, type or use and thereby afford consumers with the right to review, dispute and, where appropriate, correct information that is used to make decisions about them.

Moreover, as I have noted in testimony the sensitive nature of the information calls for this oversight to be applied to all entities who handle this data. The potential for harm is the same regardless of whether breach occurs by a company in our industry or other for-profit entities, or if such information is exposed by government, non-profit organizations or academic institutions.

Douglas C. Curling, President, ChoicePoint Inc. ("ChoicePoint" or the "Company") hereby responds to the written questions propounded by Senator Leahy in connection with the Senate Judiciary Committee's April 13, 2005, hearing on "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use." I believe the information included in the responses which follow is accurate and represents my best efforts to provide complete responses. I reserve the right to supplement or modify these answers as may be appropriate in light of information, through review of additional documents or otherwise, which may hereafter come to my attention.

1. **ChoicePoint reported in its Form 8-K filing with the U.S. Securities and Exchange Commission (SEC) on March 4, 2005, that it discovered a security breach on September 27, 2004, and that it reported this breach to the Los Angeles police.**

   a. **In a recent hearing before the California Senate Committee on Banking, Finance and Insurance Committee, Senator Jackie Speier commented that the Los Angeles sheriff's office reported to the Committee that ChoicePoint notified the sheriff's office of the breach on October 21, 2004. ChoicePoint Vice-President Don McGuffey disputed that date, citing a recollection of "the 12th or so of October." Please clarify this difference and provide the date on which ChoicePoint first contacted the Los Angeles sheriff's office regarding the security breach, and provide any documentation of that contact. In addition, please explain in detail why there was a time delay between the discovery of the breach on September 27 and notice to local law enforcement.**

The Los Angeles consumer fraud-based security breach first came to ChoicePoint's attention on September 27, 2004, when 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 prospective customer's application to ChoicePoint's Security Services Department. After a preliminary review and investigation, the manager of the Security Services Department alerted the Los Angeles County Sheriff's Department and left a message on October 13, 2004. This individual spoke to Lt. Costa of the Los Angeles County Sheriff's Department Identify Theft Task Force, explaining the situation and ChoicePoint's suspicions on October 14, 2004, and had a subsequent call with Lt. Costa on October 19, 2004. On October 21, 2004, ChoicePoint received a call from Lt. Duane Decker of the LASD Identity Theft Task Force, which was the first time anyone at ChoicePoint spoke to Lt. Duane Decker.

   b. **On what dates did ChoicePoint begin and complete notice to California residents impacted by the security breach? On what dates did**

ChoicePoint begin and complete notice to non-California residents impacted by the security breach? In addition, please explain in detail the reasons for any delays between notice to California residents and notice to non-California residents.

ChoicePoint sent notification letters to California consumers whose personal information may have been improperly accessed beginning on February 9, 2005. These mailings, which were made in two phases, were completed by February 18, 2005. Thereafter, ChoicePoint made a subsequent mailing on February 25, 2005 to California consumers. This mailing was a remailing because the initial California notifications had not included information about the Experian credit monitoring service ChoicePoint has made available to each consumer.

ChoicePoint mailed notices between February 23, 2005 and February 24, 2005 to consumers in all states other than California. ChoicePoint made a subsequent mailing nationwide on March 3, 2005 to additional consumers who had been identified by the Company as a result of its ongoing work on matters related to the consumer fraud-based security breach.

The timing of ChoicePoint's notice to consumers was impacted primarily by two factors: a) certain requests from law enforcement that notifications would impede criminal investigations. b) the sheer amount of work involved in identifying the fraudulent accounts, reviewing the log files (information captured by ChoicePoint's systems in connection with the fraudulent accounts), and attempting to replicate the searches run by the fraudulent accounts, and then identifying and notifying the relevant consumers substantially affected the timing of ChoicePoint's notice. In addition to preparing to provide notice, the Company also had to prepare a telephone center to receive calls from consumers who received notification and elected to contact the company through the established toll free number.

In connection with the Los Angeles consumer fraud-based security breach referenced above in response to Question (1)(a), ChoicePoint received a letter dated November 23, 2004 from the Los Angeles County Sheriff's Department asking it to delay notification. Towards the end of January 2005, the Company sought and obtained permission from the Los Angeles County Sheriff's Department to begin sending notifications to consumers. As noted above, the mailing of these notifications began on February 9, 2005.

It is also important to note that ChoicePoint was obligated to provide notice to California consumers only pursuant to California Civil Code § 1798.82.

c. ChoicePoint's March 4, 2005 Form 8-K filing with the SEC reported that 145,000 individuals were impacted by security lapses at ChoicePoint

between July 1, 2003 and March 4, 2005. Did ChoicePoint experience any significant security breaches prior to July 1, 2003 that resulted in unauthorized access to personal information? If so, please detail the scope and impact of those breaches, whether the affected individuals received notice, whether the affected individuals experienced identify theft as a result of the breach, and what changes ChoicePoint implemented in its policies and systems prior to July 1, 2003 in response to those breaches.

The Federal Trade Commission (FTC) is conducting an 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 the 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 those accounts have been notified. Additionally, we found an account recently that we have investigated and identified approximately 100 potentially affected consumers whom we have now notified.

ChoicePoint continues to investigate and work with law enforcement regarding the Los Angeles incident, terminating accounts and/or user names and passwords as appropriate. It should be noted that from time to time ChoicePoint receives requests for information from law enforcement – primarily in the form of subpoenas. Historically, our relationship with law enforcement has been a one-way street whereby we respond as quickly as possible with the information requested. Many times we do not gain additional information from law enforcement regarding such requests.

ChoicePoint recognizes the importance of securing sensitive data and our security processes always continue to evolve. With respect to consumers affected by the consumer fraud-based security breach that gave rise to the notifications in February and March 2005, ChoicePoint has taken a number of steps in addition to such notifications:

- First, ChoicePoint has established a dedicated toll-free customer service number and a special web site to respond to inquiries;
- Second, ChoicePoint is providing, free of charge, a combined three-bureau credit report;
- Third, ChoicePoint is 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.

In addition, ChoicePoint has strengthened its customer credentialing process and is changing its products and services to many customer segments. It is requiring additional due diligence such as banking references and site visits to customers receiving personally

identifiable information before allowing access to personally identifiable information. It is recredentialing sections of its customer base.

ChoicePoint is modifying the services that the company is delivering to its customers. ChoicePoint is also undertaking internal reviews with respect to certain products to examine information security, computer operations and other controls.

ChoicePoint has created an office of Credentialing, Compliance and Privacy that will report to the Board of Directors' Privacy Committee and be independent of ChoicePoint management. This office is led by Carol DiBattiste, previously Deputy Administrator of the Transportation Security Administration, Department of Homeland Security; former Director of the Executive Office for United States Attorneys, Department of Justice; former Principal Deputy General Counsel, Department of the Navy; former Director of the Office of Legal Education, Department of Justice; and former Assistant U.S. Attorney in Southern District of Florida with extensive experience in criminal prosecutions and compliance.

ChoicePoint has 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 liaison to law enforcement officials.

In addition, ChoicePoint has decided to exit the consumer sensitive data market not covered by the Fair Credit Reporting Act, meaning ChoicePoint will sell information products containing personally identifiable information consisting of date of birth and Social Security and drivers' license numbers only to industries 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 continues to review its responses to the consumer fraud-based security breaches that gave rise to the consumer notifications in February and March 2005, and will continue to take additional steps, as appropriate.

2. In a March 30, 2005, California state senate hearing, a victim of the recent ChoicePoint breach testified that she asked for a copy of her complete ChoicePoint file, but was twice told that she was not entitled to have this information.

a. What is ChoicePoint 's current practice with respect to allowing individuals to see the information that ChoicePoint has on them in its systems and distribute databases, including any costs or conditions of

access? Do individuals currently have a right to see *all* of the information maintained on them by ChoicePoint? If not, please explain.

ChoicePoint provides consumers with access to consumer reports and non-consumer report information through our consumer disclosure center and our Internet-based disclosure system, ChoiceTrust.com.

Pursuant to the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), ChoicePoint provides consumers, whether merely curious or affected, with access to those reports covered by such Acts. ChoicePoint's consumer reports include, in part, Motor Vehicle Records, ChoicePoint's proprietary C.L.U.E. Personal Property, C.L.U.E. Auto and Current Carrier reports, pre-employment reports, and tenant history reports.

Pursuant to the FCRA, FACT Act and certain state laws, consumers are entitled to free disclosure of their consumer file when adversely impacted by a consumer report and are further entitled to free disclosure of certain consumer reports on a periodic basis. ChoicePoint complies with these statutory mandates. In those instances when a consumer is not entitled to free file disclosure, ChoicePoint charges the statutorily mandated fee, which differs depending on the consumer's state of residence.

ChoicePoint also provides consumers with a public record report containing information derived from information contained in our core public record products. Currently, disclosure of such reports is free of charge.

ChoicePoint also offers consumers the opportunity to purchase a "self-check" report that includes information that may be included in the event a pre-employment report were ordered on such consumer. This "self-check" may include, at the request of the consumer, education and employment verification, criminal record, and sex offender status information. The cost of this report varies based upon the level of service requested.

Consumers may also purchase from ChoicePoint their insurance score. These scores are used by personal lines property and casualty insurance companies to facilitate the underwriting process. In addition, we provide consumers with information regarding the primary factors that contributed to their score, explanations of how the information may be used by insurance companies, and a copy of the underlying credit report from Equifax that was used in determining the score.

Finally, we offer consumers the ability to order through VitalChek, a ChoicePoint company, their vital records from all 50 states, including birth certificates and marriage records.

Before consumers are granted access to any of the information described above, there is some level of authentication performed, which may necessitate the provision of supporting documentation, to ensure that the person requesting the information is the consumer to whom the information sought pertains.

b. At the March 30, 2005, California senate hearing, Senator Speier asked Don McGuffey, a ChoicePoint Vice President, whether he "would be supportive of a bill that required that a consumer had access to all records that a data broker had on them and make that available to them?" Mr. McGuffey responded "Yes." In view of this exchange, would ChoicePoint support federal legislation that required data brokers to allow individuals access to *all* of the information maintained or distributed by a data broker about those individuals? If not, please explain.

We believe that giving increased oversight authority to the Federal Trade Commission (FTC) would provide consumers the assurance they deserve. We would further support extending the principles of the Fair Credit Reporting Act (FCRA) to cover all sensitive personally identifiable data regardless of its source, type or use and thereby afford consumers with the right to review, dispute and, where appropriate, correct information that is used to make decisions about them.

Moreover, as noted in my testimony the sensitive nature of the information calls for this oversight to be applied to all entities who handle this data. The potential for harm is the same regardless of whether breach occurs by a company in our industry or other for-profit entities, or if such information is exposed by government, non-profit organizations or academic institutions.

c. At the March 30, 2005, California senate hearing, Don McGuffey also testified that "in our new era, we are working today to provide a single point of contact to be able to deliver to consumers who request it, free of charge, a report that would include the variety of products and services that we have delivered and delivered today . . . . As we can get built a single point of access, a consumer will be able to see the products that they have available to them, request the products at no charge, and we will deliver them." Would this single point of contact cover any and all personally identifiable information on individuals that ChoicePoint provides to any of its customers? When does ChoicePoint expect to have such a single point of contact available to use?

As described above, ChoicePoint affords consumers the ability to request disclosure of the information outlined above through www.choicetrust.com.

3. According to a ChoicePoint news release, on December 29, 2004, ChoicePoint wrote a letter to the Electronic Privacy Information Center, stating that "ChoicePoint fully complies with the FCRA, including the new Fair and Accurate Credit Transactions Act (FACTA), where they apply to our products and services."

a. Has any court or administrative agency found ChoicePoint in violation of FCRA? If so, please detail the nature of those violations and any fines, consent decrees or other consequences of those findings.

In Boris v. ChoicePoint Services Inc., 249 F. Supp. 2d 851 (W.D. Ky. 2003), a federal district court in Kentucky upheld a jury verdict finding that ChoicePoint Services Inc. did not follow reasonable procedures to assure maximum possible accuracy as required by FCRA § 607(b) with respect to its preparation of consumer reports about the plaintiff and that ChoicePoint Services Inc. did not properly execute its reinvestigation obligations pursuant to FCRA § 611. ChoicePoint Services Inc. appealed the matter; the parties, however, settled the matter out of court prior to resolution of the appeal pursuant to a confidential settlement agreement.

b. Has ChoicePoint entered into out-of-court settlements for violation of FCRA? If so, please provide the number of occasions and the aggregate settlement amounts.

A review of company records in response to this request indicates that, in litigation initiated since ChoicePoint became an independent, publicly-traded company in 1997, ChoicePoint companies have settled nine lawsuits (including the Boris matter, discussed above) in which plaintiffs have alleged FCRA violations. These nine matters were settled for approximately $554,202.84, which in some cases included monies for attorneys' fees and costs.

June 17, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

Dear Chairman Specter:

Thank you for the recent opportunity to testify before the Committee on the Judiciary on "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use." Please find below responses to questions that you forwarded to me from Senators Leahy and Biden after the hearing.

Senator Leahy's Questions

Q1. Following the revelation of its sale of personal data to fraudulent companies, ChoicePoint announced that it would exit the consumer-sensitive data market not subject to the Fair Credit Reporting Act (FCRA), and would no longer distribute information containing social security and drivers's license numbers, except in consumer-driven transactions or where the product supports federal, state or local government and law enforcement purposes. Although ChoicePoint has exited this market, can you estimate how many other data brokers still provide products and services that they are not subjecting to the Fair Credit Reporting Act or Gramm-Leach-Bliley?

A. The FTC does not maintain information about the total number of data brokers or the products and services that they offer. Estimating the number of data brokers that are subject to specific laws is difficult because whether a data broker's products and services are subject to the FCRA or GLBA depends upon how the data products or services are used and the source of the data. For example, any data broker that provides certain information used to evaluate a consumer's eligibility for credit, a job, an apartment, or other commercial transaction is a consumer reporting

agency and subject to the FCRA. In addition, any customer information that a data broker receives from a financial institution, including a credit bureau, is protected by the GLBA Privacy Rule and cannot be further disclosed except under an exception.

Additionally, there may be data brokers that provide products or services that contain SSNs or driver's license numbers that were not obtained from a financial institution, but rather from other sources, such as public records. This information would not be regulated by the GLBA, and may not be regulated by the FCRA.

Finally, there are many data brokers that provide products and services that do not contain SSNs or driver's license numbers, such as directories that provide contact information derived from phone books and other publicly available sources.

Q2. During the April 13, 2005 hearing before the Senate Judiciary Committee, Senator Leahy asked you whether you would support the application of FCRA to data brokers. In response you stated, "I think we should look at whether some of those provisions should be applied." Please specify which FCRA provisions, with any modifications, you recommend for application to data brokers and why? If there are provisions of FCRA that you do not believe should apply to data brokers, please explain.

A. The FCRA requires that consumer reporting agencies take steps to verify the identities of their customers and the purposes for which they are requesting consumer reports. This requirement is designed to ensure that sensitive information is used only for certain purposes, and that the information does not fall into the wrong hands. As the Commission has stated in its testimony, we believe that Congress should consider requiring that all companies that handle sensitive data have reasonable and appropriate safeguards for that information. This requirement may address some of the same concerns as the verification requirements in the FCRA. For example, in the context of a data broker, we believe reasonable security would encompass reasonable steps to verify the identity of customers to whom sensitive information is sold.

The FCRA also imposes access, correction, and accuracy requirements. These are important principles to consider in any system of information regulation. To the extent certain information from data brokers is being used to make determinations about consumers' eligibility for credit, insurance, or similar business transactions, it is already subject to the FCRA. Before extending this approach to additional databases, however, it is necessary to consider carefully the impact of that extension. For example, requiring data brokers to provide consumers access to sensitive information may itself present a significant security issue – in some cases, it may be difficult for the data broker to verify the identity of someone who claims to be a particular consumer demanding to see his or

her file. Similarly, for databases that are used to prevent fraud or other criminal activities, providing correction rights could pose serious problems; those trying to perpetrate fraud may take advantage of the right to "correct" data to hide it from those they are trying to defraud. As you know, we are conducting investigations of recent data breaches and hope to learn more about the operation of these databases.

Additional Questions

Q1. Based upon the data that you have collected, what do you believe are the underlying drivers of the rise in identity theft, e.g., ease of access to information, stores of data being collected by data brokers, the reliance on credit in our monetary system? I realize that the answer will probably be a combination of many factors, but an examination of these underlying factors can assist in determining how to combat the problem, such as increased restrictions on gathering personal information, mandated data security and management practices, limits on the use of social security numbers, etc. Thus, I would appreciate your honest opinion on how we got where we are, and how we get from where we are to where we want to be with respect to this problem?

A. Data from two nationally projectable surveys published in 2003 and 2004 indicated that for the twelve months preceding the surveys, the rate of identity theft remained stable. Each year since the FTC implemented the Identity Theft Data Clearinghouse in 1999,[1] we have seen a steady increase in the number of victims reporting their identity theft complaints to the FTC.[2] This increase may reflect a greater awareness by consumers regarding the FTC's centralized complaint and victim assistance center. It does not necessarily reflect a net increase in the number of victims. Because our victim data is self-reported, in 2003 the FTC commissioned a survey that looked at the two major categories of identity theft: (1) the misuse of existing accounts; and (2) the creation of new accounts in the victim's name. The FTC survey found that nearly 10 million consumers reported discovering that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses. Victims of identity theft in both categories cumulatively reported spending almost 300 million hours

---

[1] The FTC's Clearinghouse database is the nation's centralized repository of identity theft consumer complaint data. The FTC established this law enforcement database, which facilitates cross-jurisdictional investigations, as well as the other core components of its Identity Theft Program (such as the Identity Theft Hotline, website, and consumer educational materials) in direct response to its congressional mandate under the Identity Theft and Assumption Deterrence Act of 1998.

[2] In CY 2000, the FTC received 31,123 identity theft complaints; in CY 2001: 86,212; in CY 2002: 161,836; in 2003: 214,905; in CY 2004: 246,570; and today the database contains over 860,000 identity theft complaints.

correcting their records and restoring their good names. The survey also showed a correlation between the type of identity theft and its cost to victims, in terms of both time and money spent resolving the problems. For example, while consumers who had accounts opened in their names made up only one-third of the victims, they suffered two thirds of the direct financial harm.

Identity theft is a crime of opportunity and it takes myriad forms. A thief can take over someone else's identity by stealing incoming or outgoing mail from a home mailbox or via a complex, cyber-data heist. What this means for regulators and legislators is that there is no one single approach to controlling the problem. There are ways, however, to minimize risks to data and thereby decrease opportunities for identity theft. I believe that we can move forward with respect to this crime by considering ways to make key data less easily available to commit identity theft. For example, Congress could consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to secure its safety. I also believe that if an information security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified. Prompt notice can enable consumers to take steps to protect themselves and mitigate the damage caused by identity theft.

Q2. Recent FTC statistics indicate that Americans spend up to 300 million hours cleaning up credit records damaged by identity theft. What role does the FTC play in helping citizens clean up their records? Are there any conflicts with state and federal law that makes this task harder for victims? What can the FTC do to ease the burden in restoring the credit of identity theft victims?

A. As discussed below, the Commission has a number of ongoing efforts to assist victims of identity theft and to prevent consumers from becoming victims in the first instance. I do not see conflicts between federal and state law making recovery harder for identity theft victims. Moreover, we work closely with local law enforcement agencies to support their efforts to investigate and prosecute identity theft cases.

At the FTC, we conduct education and outreach on three fronts: we provide training and investigative resources to law enforcement; we also provide targeted outreach on prevention and victim assistance to the business community; and through our toll-free Identity Theft Hotline and web services, we provide guidance and education directly to thousands of victims every week.[3] In addition, when consumers contact us to file a complaint, their complaint data is made available to authorized law enforcement

---

[3] We currently receive some 15,000-20,000 contacts per week via hotline, website, or mail. To assist victims, we have developed a brief primer on identity theft, a comprehensive victim recovery guide, and an *ID Theft Affidavit*, designed to simplify the recovery process. All these materials are also available in Spanish.

personnel through the FTC's cybertool – the Consumer Sentinel Network.[4] In this way, law enforcement officers nationwide have real-time access to this centralized complaint data, which in turn can facilitate cross-jurisdictional investigations.

Through the FTC's Identity Theft Program, victims across the country have been able to learn how to minimize their risks and what steps to take to remedy the effects of this crime. Through our partnership with law enforcement, we have facilitated training and provided investigative resources that enhance the ability of law enforcement to work within their communities to assist victims. For example, to reach local police departments, the FTC has partnered with the International Association of Chiefs of Police on several projects, and has authored articles for Police Chief Magazine, the IACP monthly publication, on tools that police departments can use in working with identity theft victims. We have also worked closely with industry to provide outreach on prevention, and ways to help consumers whose information has been misused. Of course, we encourage industry to secure individuals' personal information so as to minimize the risk of data breaches in the first instance.

---

[4] More than 1,200 law enforcement agencies have access to the ID Theft Data Clearinghouse through Consumer Sentinel.

In addition, industry has new obligations under the FACT Act[5], and they will need to work closely with victims to assist them with the recovery process.[6] The FTC will continue to support training and outreach efforts and foster continued dialogue with consumer and industry groups to ensure that we provide assistance and education that is effective.

Q3. Do you recommend any changes in federal law to make it easier on victims who suffer from identity theft?

A. Recent changes in federal law through the FACT Act amendments to the Fair Credit Reporting Act (FCRA) have made it easier for victims to remedy the effects of identity theft. For example, victims can now obtain the fraudulent transaction records from businesses that extended credit to the identity thief. In addition, under the new FCRA provisions, victims are entitled to place fraud alerts in their credit files and obtain additional free copies of their file disclosures. Victims can now also have the consumer reporting agencies (CRAs) block inaccurate information resulting from identity theft from their credit files and prevent businesses from reporting inaccurate information to the CRAs if the consumer can show it resulted from identity theft. And, when victims contact the CRAs, these companies must provide the victims with a summary of their new FCRA identity rights – this summary was drafted by the FTC in consultation with the federal banking agencies and the National Credit Union Administration. These new measures became effective last year, and I believe all these changes to federal law will further assist victims in remedying the effects of identity theft.

---

[5] Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681, *et seq.*

[6] For example, businesses must provide victims with copies of the transaction records resulting from identity theft and stop furnishing the inaccurate information resulting from the identity theft to the consumer reporting agencies.

Looking forward, I believe consideration of security measures to safeguard key data is appropriate. For example, Congress could consider whether it is appropriate to extend the FTC's Safeguards Rule to companies that are not financial institutions. In addition, should Congress decide to enact a security breach notice provision, Congress could authorize the FTC to conduct a rulemaking on this question to establish criteria under which notice would be required, which could depend on the type of breach, the risk of harm, and the appropriate form of notice. I would be happy to work with your Committee to further develop any or all of these proposals.

Senator Biden's Questions

Q1. Given the growing nature of this identity theft, the many ways that it is manifested (database intrusions, mail theft, phishing schemes), and the reliance of credit in our monetary system, it is clear that federal, state, and local law enforcement and regulatory agencies have their hands full in addressing the problem. Are the legal authorities that are currently available sufficient for you to prevent, investigate, prosecute and punish perpetrators of identity theft? Do you have sufficient resources to effectively combat identity theft?

A. The federal laws directly applicable to identity theft are the Identity Theft and Assumption Deterrence Act of 1998[7] and the Identity Theft Penalty Enhancement Act of 2004.[8] The 1998 Act defines the crime of identity theft, and the 2004 Act created an aggravated offense allowing for tougher sentences in certain situations such as when the thief obtains customer information under false pretenses (adds an additional 2 years to the sentence) or where the identity theft is related to terrorism (adds an additional 5 years). These laws give criminal law enforcement agencies the tools to investigate as well as prosecute and punish identity thieves. In addition, identity theft often violates other federal laws such as the mail and wire fraud statutes.

Criminal enforcement is handled at the federal level by the U.S. Attorneys' Offices and other criminal investigative agencies, such as the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service. In addition, because many identity thefts occur locally, state and local law enforcement agency resources also are significantly involved in addressing this problem.

---

[7] 18 U.S.C. § 1028.

[8] Pub. L. No. 108-275 (2004).

I believe the FTC has adequate resources to perform its role. Because the FTC does not enforce criminal law and because identity theft enforcement occurs at both the federal and local level, those agencies would be the most appropriate sources of information on the adequacy of their resources. The FTC, however, has taken a number of steps[9] in facilitating training and providing outreach and investigative resources to its criminal law enforcement partners, as well as in educating the public and working with industry to disseminate information on prevention and victim assistance. For example, since 2002, the FTC, in conjunction with the U.S. Department of Justice and other important partners,[10] has facilitated identity theft training seminars across the country. Since 1999, we have logged over 860,000 identity theft complaints from victims. This consumer

---

[9] The Identity Theft and Assumption Deterrence Act of 1998 directed the FTC to play a central role in the identity theft arena. Under this Act, Congress directed the FTC to log and acknowledge consumer complaints, provide informational materials, and refer complaints to appropriate entities. The components of the FTC Identity Theft Program (including a toll-free Hotline, an on-line complaint form, an Identity Theft website and consumer education materials, the Identity Theft Data Clearinghouse – a law enforcement database that can facilitate cross-jurisdictional investigations, and targeted criminal referrals) were developed in direct response to the FTC's mandate under the 1998 Identity Theft Act.

[10] The U.S. Secret Service, the U.S. Postal Inspection Service, the American Association of Motor Vehicle Administrators, and local and state law enforcement participate in the day-long identity theft training events. More than 2,550 police officers have attended these seminars, representing over 890 agencies.

complaint data is made available to authorized law enforcement personnel at the federal, state and local levels through the FTC's Identity Theft Data Clearinghouse– the nation's centralized repository of identity theft complaints.[11] In addition, FTC investigators mine the database and create targeted preliminary investigative reports that are referred to law enforcement task forces or police units who have requested specific investigative data.

---

[11] To date, more than 1,200 agencies have access to the FTC's Consumer Sentinel Network, the system that houses the Clearinghouse.

Although the FTC cannot prosecute criminal identity theft cases, we do have authority to challenge practices that place consumer data at risk. Section 5 of the FTC Act[12] provides the Commission with jurisdiction to bring actions against persons who engage in unfair or deceptive practices affecting commerce.[13] Most recently, the Commission announced a settlement with BJ's Wholesale Club, Inc., which represents the FTC's first case charging that a company's failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated the FTC Act. The Gramm-Leach-Bliley Act (GLBA) imposes privacy and security obligations on financial institutions.[14] The FTC's Privacy and

---

[12] 15 U.S.C. §45(a).

[13] A prohibited practice can include a deceptive claim that a company makes about privacy, including claims about the security they provide for consumer information. To date, the FTC has brought five cases against companies for deceptive security claims about the security they provide for consumer information. *See, e.g.,* Statement of the Federal Trade Commission Before the Committee on the Judiciary, U.S. Senate, on Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use, pp. 13-15 (April 13, 2003) *available at* http://www.ftc.gov/opa/2005/04/financialdatatest.htm.

[14] 15 U.S.C. § 6809(3)(A).

Safeguards Rules, promulgated pursuant to Title 5 of the GLBA, give consumers some control over how their personal information can be shared between unrelated entities,[15] and oblige financial institutions to have reasonable procedures to ensure the security and confidentiality of certain personal information.[16] The Fair Credit Reporting Act (FCRA) protects consumers' personal consumer report information by requiring that users of these reports have a permissible purpose before they can access this information. GLBA and FCRA protections limit how certain personal information about consumers can be accessed, used and shared with third parties. In this way, current laws help limit opportunities for identity theft.

---

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

[16] Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"). 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. *Sunbelt Lending Services*, (FTC Docket No. C-4129) (consent order); *Nationwide Mortgage Group, Inc.*, (FTC Docket No. 9319) (consent order).

The FTC's education mission and outreach efforts have targeted many sectors of the population. For example, to assist consumers, we have developed a comprehensive victim resource guide,[17] an identity theft primer,[18] a summary of the new FCRA identity theft rights entitled "*Remedying the Effects of Identity Theft*,[19] and the *Id Theft Affidavit*.[20] These educational materials are available for free (in English and Spanish) upon telephone request or via the FTC's identity theft website, at www.consumer.gov/idtheft. The Commission hosts a toll-free Identity Theft Hotline, 1-877-ID-THEFT. Callers to the Hotline receive counseling from trained personnel who provide information on prevention of identity theft, and what steps to take to resolve the problems resulting from the misuse of their identities. In addition, FTC staff regularly conduct on-site presentations to consumer and business groups on steps to take to minimize the risk of identity theft and how to remedy the effects of this crime.

I believe we have sufficient resources to allow us to disseminate information on identity theft prevention and victim assistance broadly. Our approach is to enable diverse entities – businesses, educational institutions, and many others – to use our materials to further assist affected consumers when they contact these entities and need assistance from them.

Q2. Are most of the perpetrators of identity theft domestic or foreign? What additional challenges do you face in investigating perpetrators from overseas? What efforts are currently underway to secure greater cooperation, if necessary, from foreign nations?

A. Although currently most targets of FTC privacy and security investigations are domestic, increasingly we see an international component in these investigations, where investigative targets, witnesses, evidence, affected consumers, or assets are located abroad.

To protect consumers' personal information in an increasingly global marketplace, the FTC has brought several enforcement actions with an international component. For example, we have brought enforcement actions against Canadian telemarketers engaged in the practice of "pretexting," where they obtain customer information of financial

---

[17] *Take Charge: Fighting Back Against Identity Theft.*

[18] *ID Theft: What's It All About?*

[19] Consumer reporting agencies must also provide this two-page summary to victims who contact the companies because they believe they are, or are about to become, victims of identity theft.

[20] The *ID Theft Affidavit* assists victims in reporting and disputing fraudulent tradelines.

institutions under false pretenses.[21] In addition, we have worked to build enforcement cooperation relationships with foreign authorities through bilateral and multilateral networks.

Despite these efforts, the FTC faces challenges in addressing cross-border fraud including fraud relating to privacy and security of information. One such challenge is a statutory restriction on our ability to share certain investigative information with foreign law enforcement agencies, even if such sharing would further our own investigation. The FTC has worked with Congress to develop proposed legislation that would address this challenge and others, and give the Commission new tools to protect American consumers' privacy in the global marketplace. This new legislation is important to overcoming existing obstacles to information sharing, improving the FTC's ability to gather information, enhancing the FTC's ability to take effective action in cross-border cases, and strengthening the FTC's ability to cooperate with foreign authorities.

If you or other Committee Members have any further questions, please do not hesitate to contact me. I look forward to working with you and the Committee on these issues in the future.

Sincerely,

Deborah Platt Majoras
Chairman

---

[21] *See, e.g., FTC v. Assail, Inc.*, Civ. No.W03CA007 (W.D. Tex., filed Jan. 9, 2003), *available at* http://www.ftc.gov/opa/2003/01/assailnetwork.htm; *FTC v. Millenium Mktg.*, Civ. No. 04C 7238e (N.D. Ill., filed Nov. 9, 2004), *available at* http://www.ftc.gov/opa/2004/11/millineum.htm.

Chairman Specter
Questions for Witnesses
April 13, 2005
Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Governmental Use

Questions for Kurt P. Sanford, CEO, LexisNexis, Corporate & Federal Markets

1. Your letter of April 20, 2005, described the recent breaches your company experienced and the investigations you conducted in response to those breaches. Here are some follow-up questions:

a. How did the unauthorized users obtain your customers' passwords?

The incidents involving LexisNexis and Seisint continue to be the subject of an ongoing law enforcement investigation. We will learn more about the methods used to obtain IDs and passwords from our customers as these investigations conclude. What we know at present is that several different methods were used to obtain passwords. In each instance the password was obtained from the customer. Examples include: malicious spyware placed on the computer of a customer without their knowledge to capture keystrokes entered by the customer and to download the keystrokes to the hacker; and the use of scripting techniques used to generate different passwords until the correct password is discovered.

b. What will LexisNexis/Seisint do to prevent future breaches?

We have learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. These include:

- Changing customer password security processes to require that passwords for both system administrators and users with access to sensitive personal information be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;
- For customers with access to sensitive personal information, suspending customer login IDs after five unsuccessful login attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation;
- Further limiting access to the most sensitive data in our databases by truncating SSNs displayed in non-public documents and narrowing access to full SSNs and DLNs to law enforcement clients and a restricted group of legally authorized organizations, such as banks and insurance companies; and
- Educating our customers on ways they can increase their security.

c. Prior to the recent revelations regarding breaches at LexisNexis/Seisint and other companies, what steps did LexisNexis take when it discovered a breach involving personal information?

Prior to the recent security incidents, LexisNexis routinely monitored usage patterns and in instances where customer usage patterns were inconsistent with normal search patterns or followed a pattern of known system abuse, LexisNexis would cut off access to the affected user ID(s), accounts or Internet addresses and investigate the incident further.

2. Have any affected consumers ever sued LexisNexis or Seisint for damages caused by a breach? If so, please describe the substance of each suit and its outcome or current status.

In April 2005, a purported class action captioned *Syran v. LexisNexis Group, et. al.*, Case No. 05 CV 0909 LAB (POR), was filed in the United States District Court for the Southern District of California. The lawsuit names Reed Elsevier, Inc., LexisNexis Group, and Seisint, Inc. as defendants and claims violations of the federal Fair Credit Reporting Act, the California Information Practices Act, the California Consumer Credit Reporting Agencies Act, the California Investigative Consumer Reporting Agencies Act, and the California Unfair Competition Law based on Defendants' alleged failure to maintain reasonable procedures to protect consumer credit information from unauthorized access by third parties. No proceedings relating to this purported class action have yet occurred. The plaintiffs seek unspecified punitive and statutory damages, attorneys' fees and costs, and injunctive relief. We believe we have strong defenses to this action and will vigorously pursue them.

A second suit has recently been filed in the United States District Court for the Northern District of California. The named plaintiff is Mark Witriol. The complaint is similar to that filed in *Syran*.

3. How do you ensure that the data you collect, maintain and sell is accurate? How accurate do you think the data is?

LexisNexis employs a number of procedures to test the accuracy of the information we receive and to test the accuracy of this data prior to making the data available to customers. The data conversion process is itself subject to a series of system checks. The data is run through the conversion process where computer systems and software check for conformance with formatting specifications. Deviations, anomalous data, and data omissions are noted and brought to the attention of the appropriate LexisNexis personnel for verification, review, or remediation with the data supplier.

LexisNexis obtains data only from known, reputable sources.

- We receive the most current data that the supplier can provide;
- Any questions arising regarding the accuracy of the content delivered to LexisNexis are resolved quickly and effectively;
- Data is delivered in the same, mutually agreed upon format, thereby maintaining the integrity of the data conversion process and minimizing the risk of conversion errors;
- We respond to any questions regarding data accuracy brought to our attention by consumers or others; and
- Any updates, additions, or changes are received from the supplier.

4. What is the universe of personal data contained in LexisNexis/Seisint's databases? What are the specific sources of this data?

Sensitive personal data contained in the LexisNexis and Seisint databases is limited to social security numbers (SSNs) and driver's license numbers (DLNs). The source of SSNs is credit header data obtained from credit bureaus. Credit header data is the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, SSN, and month and year of birth. DLNs are obtained from state Departments of Motor Vehicles. Other types of information available on LexisNexis and Seisint are identified on the attached list. (Attachment A.) These data types are obtained primarily from federal, state, and local government offices and courts. The documents are in most instances public records made available to the public under applicable open record laws. Covered offices include: secretaries of state; county recorders; county tax assessors; federal courts; state courts; county and municipal courts; and court clerks.

Some record types come from privately published, public sources such as white page telephone directories, professional directories, credit headers, and Dun & Bradstreet reports.

5. Please identify specifically which types of personal data collected, held or sold by LexisNexis/Seisint, or transactions offered by LexisNexis/Seisint, are regulated by FCRA?

LexisNexis/Seisint provides specialized products that are regulated under the FCRA. These products are used for employment screening and tenant screening. Separate databases are maintained for FCRA regulated products.

a. Please identify which provisions of FCRA apply to each type of data or transaction?

The FCRA applies only to those LexisNexis/Seisint products that include information that bear on one or more of the seven FCRA factors *and* which are used by our

customers for an FCRA permissible purpose. Examples of our products that are governed by the FCRA are our products that are used for employment and tenant screening purposes. None of LexisNexis/Seisint's business operations qualify as Nationwide Consumer Reporting Agencies. The Nationwide Specialty Consumer reporting Agency rules do apply to one of LexisNexis/Seisint's business operations.

b. Of the personal data that LexisNexis/Seisint collects, maintains or sells, and the transactions offered by LexisNexis/Seisint, which are not regulated by FCRA?

The information contained in the general LexisNexis and Seisint databases are not regulated under the FCRA. However, LexisNexis and Seisint provide specialized products that are regulated under the FCRA as referenced in our response to question 5 above.

c. FCRA requires that you always notify individuals when you report adverse information about them on an employment check. Do you always do this?

Yes. LexisNexis/Seisint complies fully with this requirement.

6. What language would you recommend Congress adopt requiring companies like yours to give notice when they experience a breach?

LexisNexis supports requiring notification in the event of a security breach of computerized data involving sensitive personal information where the breach results in a significant risk of identity theft resulting in economic harm. Care should be taken to avoid a standard that requires over notification since this will lead consumers to ignore those notices that warn them of significant risks.

"Sensitive personal data" should be defined as name linked to:

- Social security number;
- Driver's license number; or
- Financial account number or credit card or debit card number, linked with any required security code, access code or password that will allow access to that account.

The following should be exempted from the definition of "sensitive personal data:"

- Encrypted or truncated data; and
- Public record information or publicly available information.

Security breach notification legislation should be promulgated as a national standard, not as a floor which would allow each state to adopt different standards. The confusion among consumers from the likely range of state requirements would

be significant, particularly where individuals involved in the same incident are treated differently. Clear federal preemption coupled with federal enforcement will help ensure uniformity of standards and will allow companies to quickly and effectively notify affected individuals.

Written Questions of Senator Patrick Leahy
For Submission in the Hearing on:

"Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use"

Before the Senate Committee on the Judiciary
April 13, 2005

Kurt P. Sanford, President and CEO, U.S. Corporate & Federal Markets, LexisNexis

1. Recently, during a March 30, 2005, California senate hearing, Don McGuffy, a Vice president at ChoicePoint, testified that "in our new era, we are working today to provide a single point of contact to be able to deliver to consumers who request it, free of charge, a report that would include the variety of products and services that we have delivered and delivered today....As we can get built a single point of access, a consumer will be able to see the products that they have available to them, request the products at no charge, and we will deliver them."

Does LexisNexis currently have such a single point of contact to allow individuals to access any personally identifiable information that LexisNexis provides on them to its customers? If not, will LexisNexis join Choice Point in committing to create such a single point of contact? If LexisNexis will not make such a commitment, please explain why not.

The LexisNexis Consumer Access Program, discussed in more detail in question 2, below, provides consumers with a single point of contact to obtain copies of report products from both LexisNexis and Seisint.

2. What is LexisNexis current policy with respect to allowing individuals to see the information that LexisNexis has on them in its systems and distributed databases, including any costs or conditions of access? Do individuals have a right to see *all* of the information maintained on them by LexisNexis? If not, please explain.

Upon request, LexisNexis will provide individuals with a copy of the information about themselves contained in the person report products distributed through the LexisNexis and Accurint information services. A person report includes public record, non-public information, and publicly available information. Public records are those records created and maintained by government agencies and are open for public inspection such as real estate title records, liens, death records, and motor vehicle registrations. Non-public information is information about an individual obtained from a source that is privately owned and is not available to

the general public. Publicly available information is information about an individual that is available to the general public from non-governmental sources such as telephone directories. There is a charge of $8.00 for this service

Some publicly available information such as news stories and magazine articles are not contained in person reports. Due to the nature of these materials they cannot be reliably matched or attributed to specific individuals via existing computer technology for inclusion in person reports. These materials are generally available to consumers through public websites over the Internet, public libraries, and bookstores.

3. On April 20, 2005, Wired News reported an announcement by Rapsheets – a division of ChoicePoint, that, whenever one of its customers runs an individual background search on its database for employment or volunteer screening purposes, Rapsheets will notify the individual and provide him or her with a copy of the background report and the name and address of the organization conducting the search, if that search reveals a criminal record. Does LexisNexis currently have a similar policy? If not, will LexisNexis provide individuals such information in the future? If so, when, and if not, why not?

LexisNexis specialized products used for employment screening are regulated under the FCRA. Section 613 of the FCRA mandates that when a regulated entity provides potentially adverse public record information (such as arrests, convictions, and bankruptcies) from its files for employment purposes, the regulated entity must notify the consumer via first class mail that it is furnishing the public record information to an end user and provide the consumer with the name and address of the end user to whom such information is being furnished. The regulated entity must inform the consumer they are entitled to receive a copy of the information being furnished, and how to dispute the information if it is incorrect. LexisNexis/Seisint is in compliance with this requirement.

Attachment A

Available Record Types in LexisNexis and Seisint Databases

1. Credit Headers*
2. Telephone Directories*
3. Professional Directories*
4. FAA Aircraft
5. Merchant Vessels
6. Property Deeds
7. Property Assessments
8. Motor Vehicles
9. Boats
10. Delaware Corporations
11. Dun & Bradstreet*
12. Internet Domains*
13. UCC Filings
14. Corporation Filings
15. Sex Offender Registry
16. County Arrest Records
17. County Court Records
18. State Court Records
19. Department of Corrections
20. Tax Liens & Judgments
21. Foreclosures
22. Marriages/Divorces
23. Florida Accidents
24. Civil Court
25. Bankruptcy
26. DEA Controlled Substances
27. Federal Firearms & Explosives
28. Voter Registration
29. Concealed Weapons Permits
30. Hunting/Fishing Licenses
31. FAA Pilots
32. Professional Licenses
33. Driver Licenses
34. Driving History Records
35. OFAC & Export Admin. Denied Persons

* Information generated by non-government entities.

SUBMISSIONS FOR THE RECORD

WRITTEN TESTIMONY OF

JENNIFER BARRETT
CHIEF PRIVACY OFFICER
ACXIOM CORPORATION

BEFORE THE
UNITED STATES SENATE
JUDICIARY COMMITTEE

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

APRIL 13, 2005

Written Testimony of Jennifer Barrett
Acxiom Corporation
April 13, 2005

Introduction

Chairman Specter, Senator Leahy, and distinguished Members of the Committee, thank you for holding this hearing and taking the time to explore the balance between protecting privacy and the beneficial uses of information by the commercial sector and the government. Acxiom appreciates the opportunity to participate in today's hearing.

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

It is important that we all recognize that information has become an ever growing and ever more integral part of the American economy. As such, we believe that it is Acxiom's solemn obligation to provide effective safeguards regardless of the difficulties encountered in doing so.

Let me be blunt. The bad guys are smart and getting more organized. They will use all of the skills available to them to try to find ways to obtain the information they need to commit fraud. Acxiom must therefore remain vigilant and innovative, and that is why we employ a world-class information security staff to help us fend off criminals who attempt to access Acxiom's data. Acxiom is constantly improving, auditing and testing its systems. Yes, Acxiom is even learning from security breaches when they occur, and we are certain that other responsible companies are doing so as well.

As Chairman Deborah Majoras of the Federal Trade Commission recently stated in her testimony before the Senate, "[T]here is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." Even though we believe that this is true, no one has a greater interest than Acxiom in protecting information because the company's very existence depends on securing personal information pertaining to consumers.

In order to enjoy the benefits provided by a robust information-based economy and also to keep our citizens safe from fraudulent activity, we believe that it is necessary that cooperation exists among policy makers, information service providers, Acxiom's clients, law enforcement and consumers. We applaud your interest in exploring these issues and we very much want to be a resource in helping you achieve the proper legislative balance we all seek.

About Acxiom Corporation

Founded in 1969, Acxiom is headquartered in Little Rock, Arkansas, with operations throughout the United States, including Arkansas, Illinois, Arizona and Ohio. The company also has offices in nine other countries across Europe and Asia. From a small company in Arkansas, Acxiom Corporation has grown into a publicly traded company with more than 6,000 employees worldwide

Acxiom's U.S. business includes two distinct components: customized computer services and a line of information products. Acxiom's computer services represent the vast majority of the company's business and they include a wide array of leading technologies and specialized computer services focused on helping clients manage their own customer information. These services are offered exclusively to large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under state and federal law. Finally, Acxiom helps government agencies improve the accuracy of the personal information they currently hold.

The balance of Acxiom's business comes from information products that are comprised of four categories: fraud management products, background screening products, directory products and marketing products. These four product lines represent less than 20 percent of the company's total business and the fraud management and background screening products represent less than 10 percent. While each product plays a unique role, all of Acxiom's information products help fill an important gap in today's business-to-consumer relationship.

To understand the critical role Acxiom plays in facilitating the nation's economy and safeguarding consumers, it is important to understand what the company *does not* do. Over the years, a number of myths have developed about Acxiom that require clarification. Please allow us to set the record straight:

- Acxiom *does not* maintain one big database that contains detailed information about all individuals. Instead, the company safeguards discrete databases developed and tailored to meet the specific needs of Acxiom's clients – entities that are appropriately screened and with whom Acxiom has legally enforceable contractual commitments. I cannot call up from the company's databases a detailed dossier on myself or any individual.

- Acxiom *does not* provide information on particular individuals to the public, with the exception of Acxiom's telephone directory products. These products, which are available on several Internet search engines, contain already public information. The other information Acxiom processes is provided only to legitimate businesses for specific legitimate business purposes.

- Acxiom's *does not* have any information in either its directory or marketing products which could be used to commit identity fraud. Acxiom also *does not* include detailed or specific transaction-related information, such as what purchases an individual made on the Internet or what websites they visited. The company's directory products include only name, address and telephone information. The company's marketing products include only information that is general in nature and not specific to an individual purchase or transaction.

- Acxiom *does not* commingle client information that the company processes in its computer services business with any of our information products. Such

activity would constitute a violation of the company's services contracts with those clients and a violation of consumer privacy. A client for whom the company performs services may have a separate agreement with us as a data contributor, but these two relationships are kept entirely separate.

Acxiom's fraud management products are sold exclusively to a handful of large companies and government agencies – they are not sold to individuals. The company's verification services only validate that the information our client has obtained from the consumer is correct. Only law enforcement and the internal fraud departments of large financial institutions and insurance companies have access to additional information.

Acxiom's background screening products utilize field researchers who do in-person, real-time research against public records and make calls to past employers to verify the information provided by the consumer. Where permitted by law, a pre-employment credit report can also be obtained. Acxiom does not pre-aggregate information for these products.

Respecting and Protecting Consumers' Privacy

Acxiom has a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. The company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security policies and privacy practices. There are, as explained below, numerous laws and regulations that govern our business. Ultimately, however, Acxiom's own comprehensive approach to information security goes far beyond what is required by either law or self-regulation.

Safeguards Applicable to Products Involving the Transfer of Sensitive Information

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law, regulations and our own company policies that help protect against identity fraud. These legal protections and additional safeguards are addressed below:

GLBA, DPPAs, and FTC: Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both state and federal driver's privacy protection acts (DPPAs). These obligations include honoring GLBA and DPPA notice and choice related to sharing and use of the information, the GLBA Safeguard Rules and FTC Privacy Rule and Interagency Guidelines. Any uses of data must fall within one of the permitted uses or exceptions specified in these laws.

FCRA and FACTA: Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). These protections include: the requirement that a consumer authorize the creation of employment reports; notice of adverse actions taken based on such report; and the right of consumers to obtain a copy of such reports and to dispute inaccuracies.

Finally, such regulations require that re-verification or correction of disputed information be performed in a timely manner.

Safeguarding Public Record Information: Public records are used in *both* Acxiom's fraud management and background screening products. Although a heightened level of protection is not mandated for such public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Safeguards Applicable to Other Products

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected, and voluntary compliance with those laws to which our clients themselves are subject.

Telephone Directory Safeguards: Acxiom's directory products comply with all applicable policies regarding unpublished and unlisted telephone numbers and addresses. In addition, because Acxiom recognizes that consumers may object to having published listings being available on the Internet, Acxiom *itself* offers an opt-out from such use. Further, Acxiom voluntarily suppresses all telephone numbers found on the Federal Trade Commission's Do-Not-Call Registry and the eleven other state Do-Not-Call registries, when providing phone numbers for targeted telemarketing purposes.

Marketing Product Safeguards: Acxiom's marketing products comply with all the self-regulatory guidelines issued by the Direct Marketing Association. These requirements include notice and the opportunity to opt-out. Consumers have the ability to opt-out from Acxiom's marketing products by calling the company's toll-free Consumer Hotline, accessing its Website, or by writing to the company. Since Acxiom does not have a customer relationship with individual consumers, Acxiom coordinates with its industry clients to research and resolve consumer inquiries.

Additional Safeguards

Acxiom takes seriously its responsibility to assure that all the information we bring to market is appropriate for the use to which it is intended and to provide adequate safeguards specifically aimed at protecting against unauthorized use.

Privacy Policy / FTC Jurisdiction: Since 1997, long before it was a common practice, Acxiom has posted its privacy policy on the company's website. The privacy policy describes both Acxiom's online and offline consumer information products. The policy further describes: what data Acxiom collects for these products; how such data is used; the types of clients to which such data is licensed; as well as the choices available to consumers as to how such data is

used. By making these extensive disclosures, Acxiom has voluntarily subjected itself to Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive conduct in the course of trade or commerce, as well as various state statutes governing unfair and deceptive acts and practices.

Consumer Care Department / Consumer Hotline: Acxiom maintains a Consumer Care Department led by a Consumer Advocate whose team interacted with more than 50,000 consumers in the past 12 months by way of answering questions, resolving issues, processing opt-outs, and handling requests for access to Acxiom's fraud management, background screening, directory and marketing products. Acxiom provides consumers who contact the company (through the company website, or by calling a toll-free Consumer Hotline or by writing to the company) the options of: opting-out of all of Acxiom's marketing products; receiving an information report from the company's fraud management and directory products; or receiving a consumer report as specified in the FCRA from the company's background screening products. Acxiom encourages consumers to notify the company if the information in any of these reports is inaccurate and it is the company's policy either to correct the information, to delete it or to refer the consumer to the appropriate source to obtain the requested correction, such as a county or state agency.

Certification and Compliance with Federal and State Law: Acxiom's privacy policy is designed to adhere to all Federal, State, and local laws and regulations on the use of personal information. The company is also certified under the Department of Commerce's European Union Safe Harbor and the Better Business Bureau's Online Seal.

Consumer Education: Acxiom believes that consumers should be educated about how businesses use information. To that end, Acxiom publishes a booklet, entitled "*Protecting Your Privacy in the Information Age - What Every Consumer Should Know About the Use of Individual Information*," which is available for free both on the company's website and upon written or telephone request.

Voluntary Acxiom Policies: Above and beyond the industry-accepted guidelines with which Acxiom complies, Acxiom also has established its own internal guidelines, which are more restrictive than industry standards. For example, Acxiom only collects the specific information required to meet its clients' information needs, and the company properly disposes of the remaining data, when information is compiled from public records. Acxiom has also implemented specific guidelines regarding the use and protection of information that could be involved identity fraud, such as Social Security numbers.

Information Practice and Security Audits: Acxiom has had a longstanding focus on the appropriate use of information in developing and delivering its information products. While the creation of strong information use policies is a business imperative, assuring these policies are followed is equally important. To this end, all of Acxiom's information products and practices have been internally and externally audited on an annual basis since 1997.

Since many of Acxiom's computer service clients are financial institutions and insurance agencies, Acxiom has been regularly audited for many years by these clients. Furthermore, Acxiom must honor the safeguards and security policies of the company's clients. Since Acxiom's security program is enterprise-wide, it is the company's policy to institute these high levels of protection across all lines of business. These client audits, along with Acxiom's own internal security audits, provide Acxiom with regular and valuable feedback on ways to stay ahead of hackers and fraudsters who may attempt to gain unauthorized access to Acxiom's systems.

Lessons Learned

Two years ago, Acxiom experienced a security breach on one of the company's external file transfer protocol servers. The hackers were employees of an Acxiom client and a client's contractor. As users with legitimate access to the server, the hackers had received authority to transfer and receive their own files. The hackers did not penetrate the firewalls to Acxiom's main system. They did, however, exceed their authority when they accessed an encrypted password file on the server and successfully unencrypted about 10 percent of the passwords, which allowed them to gain access to other client files on the server. Fortunately, the vast majority of the information involved in this incident was of a non-sensitive nature.

Upon learning of the initial breach from law enforcement, Acxiom immediately notified all affected clients and, upon further forensic investigation, the company informed law enforcement regarding the second suspected security incident. Fortunately, law enforcement was able to apprehend the suspects, recover the affected information and ascertain that none of the information was used to commit identity fraud. One of the hackers pled guilty and was sentenced last week to 48 months in federal prison. The other is currently awaiting trial.

As a result of the breach, Acxiom cooperated with audits conducted by dozens of its clients, and both the Federal Trade Commission and the Office of the Comptroller of the Currency examined Acxiom's processes to ensure that the company was in compliance with all applicable laws and its own stated policies.

This experience taught Acxiom additional valuable lessons regarding the protection of information. For example, Acxiom now requires the use of more secure passwords on the affected operating system. The process for transferring files has been changed, specifically by keeping information on the server for much shorter periods of time. And while it was always a recommended internal policy, Acxiom now requires that all sensitive information passed across such servers be encrypted. In addition, while Acxiom has had in place a Security Oversight Committee for many years, the company has also now appointed a Chief Security Officer with more than 20 years of IT experience. In short, Acxiom's systems are more secure today as a result of the company's experience and dedication to the privacy of consumers.

The Need For Additional Legislative Safeguards

There has been much discussion, especially in recent weeks, about whether existing federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored legislation would assist Acxiom and the rest of the information services industry in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

> **Breach Notification:** Acxiom supports efforts to pass federal preemptive legislation requiring notice to consumers in the event of a security breach, where such breach places consumers at risk of identity theft or fraud. California implemented similar legislation several years ago, and a number of other states are involved in similar efforts. The bottom line is that consumers deserve a nationwide mandate that requires that they be notified when they are at risk of identity theft, so they can take necessary steps to protect themselves.
>
> **Extension of the GLBA Safeguards Rule:** Currently, Acxiom voluntarily subjects itself to the GLBA Safeguards Rule with respect to the company's computer services and information products. Acxiom also complies with the California safeguards law (AB 1950). FTC Chairman Majoras recently has proposed an extension of the GLBA Safeguards Rule to the information services industry as a whole. Acxiom supports her recommendation.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing and to assist Congress in identifying how best to safeguard the nation's information and data. Acxiom is available to provide any additional information the Committee may request.

Consumers Union

West Coast Office
1535 Mission St., San Francisco, CA
94103
415-431-6747 (phone) 415-431-0906

March 29, 2005

U.S. Senator Diane Feinstein
331 Hart Senate Office Building
Washington, DC 20510

Dear Senator Feinstein:

Consumers Union, the non-profit independent publisher of *Consumer Reports* ®, strongly supports Senator Feinstein's bill, announced March 29, 2005, to require persons and government agencies who maintain sensitive information about consumers to inform consumers when the security of that information has been compromised. This measure is intended to replace the previously introduced S. 115.

This bill is an important response to rampant identity theft. Identity theft is the fastest growing form of financial fraud in the U.S. and ruins the credit of millions of Americans every year. According to a report by the Federal Trade Commission in 2003, nearly 10 million Americans were victimized by identity theft every year. That means 19 new identity theft victims in the U.S. every minute. Overall, more than 33 million Americans, about one in six adults, have had their identities used by someone else sometime since 1990. The financial costs are high. Identity theft costs consumers and businesses a staggering $51 billion annually.

The first quarter of 2005 has been filled with disturbing revelations about breaches of the security of information about consumers, including disclosures by ChoicePoint, Lexis Nexis, and others. Security breaches place individuals at increased risk of identity theft, yet only one U.S. state presently requires businesses and government entities who discover such incidents to notify the affected individuals. When ChoicePoint first announced in early February that the personal and financial information of approximately 145,000 consumers was accessed by thieves through its databases, it didn't plan to notify affected consumers in other states. After the Attorneys General from 38 states demanded equal treatment of their constituents, ChoicePoint notified affected consumers nationwide.

It shouldn't be left up to a company that has had its security breached to decide whether to tell consumers about it, or which consumers to notify. Federal law should require that all consumers be told. Senator Dianne Feinstein's proposal will accomplish this. The measure sets forth a strong, simple rule requiring notice. It has no special rules or special exceptions for some types of private entities. The bill does not let a business that has allowed a consumer's information to be seen by a crook decide whether or not to inform the consumer about the security breach.

A strong notice of security breach law gives consumers important information at a time when they can use it to attempt to reduce the damage from identity theft through early discovery. A comprehensive requirement to notify individuals of security breaches may also create a significant incentive for businesses to review and strengthen their security procedures, so that they will not experience a breach and have to disclose that breach to their customers. Finally, this measure aids identity theft victims by giving them access to the extended fraud alert when they have received notice of a security breach. This will relieve those consumers of the need to keep renewing an initial fraud alert every 90 days, which is the only remedy available to them under current law.

There is broad public demand for laws requiring notice of security breaches. AT least twenty state legislatures are considering such provisions this year. In addition to this bill, Consumers Union also supports other state and federal measures to address identity theft, including federal efforts to impose security standards and fair information practices on information brokers, restrictions on the sale, sharing, use and posting of social security numbers by private and government entities, and broader consumer privacy protections. Senator Feinstein's measure to impose a strong notice of security breach requirement is an important part of the package of new laws that are essential to stamping out identity theft stemming from theft of information from businesses or government.

For these reasons, Consumers Union is pleased to strongly support the Notification of Risk to Personal Data Act offered by Senator Feinstein.

Very truly yours,

Gail Hillebrand

Testimony of Douglas C. Curling,
President and Chief Operating Officer
Before the U.S. Senate Committee on the Judiciary
April 13, 2005

Chairman Specter, Senator Leahy and Members of the Committee:

Good morning, I'm Doug Curling, President and Chief Operating Officer of ChoicePoint.

At ChoicePoint, we recognize that in an increasingly risky world, information and technology can be used to help create a safer, more secure society. At the same time, we know, and have been painfully reminded by recent events, that there can be negative consequences to the improper access to personally identifiable data.

On behalf of ChoicePoint, let me again offer our sincere apology to those consumers whose information may have been accessed by the criminals who perpetrated this fraud. As a result of these experiences, we've made fundamental changes to our business model and products to prevent this from happening in the future. I will share details of these actions in a moment.

First, however, I'd like to share with you a little background about our company. ChoicePoint is a leading provider of identification and credential verification services to businesses, government, and non-profit organizations. We have 5,000 associates in 60 locations. We serve more than 7,000 federal, state and local law enforcement agencies, as well as a

significant number of Fortune 500 companies, more than 700 insurance companies and many large financial services institutions.

The majority of transactions our business supports are initiated by consumers. Last year, ChoicePoint helped over 100 million American consumers secure home and auto insurance. We also helped more than 7 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.

In addition to helping consumers, we're also proud of our role in helping law enforcement officials solve crimes, including the identification of the D.C.-area snipers. ChoicePoint helps agencies at all levels of government fulfill their mission to safeguard our country and its citizens.

Our products and services are also used by many non-profit organizations. For example, we have identified 11,000 undisclosed felons among those volunteering or seeking to volunteer with the nation's leading youth organizations. In addition, using information and tools supplied by us, the National Center for Missing and Exploited Children has helped return more than 800 children to their loved ones.

Mr. Chairman, apart from what we do, I also understand that the Committee is interested in how our business is regulated by federal legislation as well as various state regulations, including the Fair Credit Reporting Act (FCRA) and the recently enacted companion FACT Act, the

Gramm-Leach-Bliley Act (GLB), and the Drivers Privacy Protection Act (DPPA).

- Approximately 60 percent of ChoicePoint's business is driven by consumer initiated transactions, most of which are regulated by the FCRA. These include pre-employment screening, auto and home insurance underwriting services, tenant screening services, and facilitating the delivery of vital records to consumers.
- Nine percent of ChoicePoint's business is related to Marketing Services, none of which include the distribution of personally identifiable information. Even so, we are regulated by state and federal "do not mail" and "do not call" legislation and, for some services, the FCRA.
- Five percent of ChoicePoint's business is related to supporting law enforcement agencies in pursuit of their investigative missions through information and data services.
- Six percent of our business supports law firms, financial institutions and general business to help mitigate fraud through data and authentication services.
- The final 20 percent of our business consists of software and technology services that do not include the distribution of personally identifiable information.

Financial and identity fraud is a rapidly growing and costly threat to our nation's economy. While we offer a wide range of tools to help avoid fraud, no one is immune to it, as we and other companies and institutions are learning.

ChoicePoint has previously provided Congress with information about how identity thieves in California were able to access our products. As you know, California has been the only state that requires consumers to be notified of a potential breach of personally identifiable information. We not only followed California law, we built upon it and voluntarily notified consumers who may have been impacted across the country, and we did that *before* anyone called upon us to do so. We've also taken other steps to help assist and protect the consumers who may have been harmed in this incident.

First, we've arranged for a dedicated Web site and toll-free number for affected consumers where they can access additional information and take advantage of a range of tools not required by any federal or state law;

Second, we're providing, free of charge, a 3-bureau credit report; and

Third, we're providing, free of charge, a one year subscription to a credit monitoring service.

In addition to helping those affected consumers, we've taken strong remedial action and made fundamental changes to our business and products:

- 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.

- Second, we've strengthened ChoicePoint's customer credentialing process. We are requiring additional due diligence such as bank references and site visits before allowing businesses access to personally identifiable information. We're re-credentialing broad sections of our customer base, including our small business customers.
- Third, we've 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 out-going 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.
- Fourth, we've 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.

Let me close by speaking about the issues that must be addressed as we seek to balance the security of consumer information against the legitimate needs of business and government.

Let me be clear and unequivocal:

1. We support increased resources for law enforcement efforts to combat identity theft and stronger penalties for the theft of personally identifiable data.
2. We support independent oversight and increased accountability for those who handle sensitive personal data, including public record data;
3. We support a preemptive national notification law;
4. Finally, we support providing consumers with the right to access and question the accuracy of public record information used to make decisions about them.

I appreciate the opportunity to appear before you today and would be pleased to answer any questions that you might have.

Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
Senate Committee on the Judiciary

Securing Electronic Personal Data:
Striking a Balance Between Privacy and Commercial and Governmental Use

April 13, 2005

Chairman Specter, Senator Leahy, and Members of the Committee, thank you for the opportunity to testify today. Recent security breaches at a range of companies and institutions resulting in the loss of sensitive personal information have highlighted the need for a more substantial legal framework at the national level for entities collecting, using and selling personal data. A range of harms, including identity theft, can flow from the failure to protect electronic personal data and from governmental or corporate misuse of data or reliance on inaccurate data. We offer here today an overview of the policy landscape and suggest some approaches that Congress should consider to ensure the appropriate level of security and privacy protection. We look forward to working with you and interested stakeholders to achieve balanced solutions.

THE NEW MARKETPLACE FOR PERSONAL DATA

In the past decade, the commercial collection and sale of personal information has changed dramatically, driven by a combination of factors, facilitated by the Internet, and

[1] The Center for Democracy & Technology (CDT) is a non-profit public interest organization dedicated to promoting privacy and other democratic values for the new digital communications media. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

resulting in an ever more rapid flow of sensitive personal information in ways that most consumers barely understand. The implications for commerce, national security and personal privacy have been detailed in recent books such as Robert O'Harrow's "No Place to Hide."

The private sector and the federal government have many legitimate needs for personal information, and the sharing of data offers benefits to consumers in the form of readily available credit. Businesses and non-profit entities, ranging from landlords to retailers to lawyers to universities, obtain and share personal information to provide services and facilitate economic transactions. Indeed, an important use of commercial data services is for anti-fraud purposes, including the prevention of identity theft. The federal government uses personal information to determine eligibility for government benefits, to support law enforcement, and to fight the war on terror.

An important category of this information is drawn from public records at courthouses and other government agencies. Data brokers (we use the term throughout our testimony for lack of a better one, without intending to be derogatory and recognizing that it is not well-defined) add considerable value by aggregating and categorizing this information to provide a more complete picture of the individuals to whom it pertains.

While data brokers provide important services to the government and the private sector, they also raise a host of privacy issues and concerns about the security of this information. The recent security breaches at ChoicePoint and LexisNexis have prompted calls for examination of this new industry. Already-regulated entities, such as Bank of America, have also lost control of sensitive personal information. So have merchants whose primary business is not data aggregation. DSW Shoe Warehouse, a chain of shoe

retailers, announced recently that someone had stolen customers' credit card information from its database. And the *New York Times* reported that already this year nine universities have reported the loss or compromise of sensitive personal information.[2] Precisely because databases of electronic personal data have tremendous value, they are attracting identity thieves.

Even legitimate uses of personal data can result in harm to individuals. For instance, individuals can suffer adverse consequences when data brokers sell inaccurate or incomplete information that results in the loss of employment opportunities. In the context of government use of personal information, adverse consequences could include being suspected of criminal or terrorist activity.

Congress has addressed privacy and security issues with respect to credit reporting agencies in the Fair Credit Reporting Act (FCRA), financial institutions in Gramm-Leach-Bliley (GLB), and health care providers in the Health Insurance Portability and Accountability Act (HIPAA). But Congress's sectoral approach to information privacy has left gaps in the coverage of the law.

OVERVIEW OF POLICY RESPONSES

We see at least five sets of issues facing Congress at this time:

1. As a first step towards preventing identity theft, entities, including government entities, holding personal data should be required to notify individuals in the event of a security breach.

2. Since notice only kicks in after a breach has occurred, Congress should require entities that electronically store personal information to implement security safeguards, similar to those required by California AB 1950 and the regulations under Gramm-Leach-Bliley.

---

[2] Tom Zeller, Jr., *Some Colleges Falling Short In Data Security*, New York Times, Apr. 4, 2005, at B1.

3. Congress should impose tighter controls on the sale, disclosure and use of Social Security numbers and should seek to break the habit of using the SSN as an authenticator.

4. Congress should address the federal government's growing use of commercial databases, especially in the law enforcement and national security contexts.

5. Finally, Congress should examinee the "Fair Information Practices" that have helped define privacy in the credit and financial sectors and adapt them as appropriate to the data flows of this new technological and economic landscape.

WHAT IS PRIVACY?

Information privacy is not merely about keeping personal information confidential. Rather, it is well established by United States Supreme Court cases, the federal Privacy Act, and privacy laws like the FCRA and HIPAA that the concept of privacy extends to information that an individual has disclosed to another in the course of a commercial or governmental transaction and even to data that is publicly available.[3] Information privacy is about control, fairness, and consequences. Data privacy laws limit the use of widely available, and even public, information because it is recognized that individuals should retain some control over the use of information about themselves and should have redress to the consequences that result from others' use of that information. A set of

[3] In United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 762–63 (1989), the Supreme Court rejected the "cramped notion of personal privacy" that "because events . . . have been previously disclosed to the public, . . . [the] privacy interest in avoiding disclosure of a . . . compilation of these events approaches zero." The Court held in that case that the government can withhold from public disclosure databases composed entirely of publicly available data because there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information . . . and revelation of the [information] as a whole." The Court based its ruling on the conclusion that, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." 489 U.S at 764. The Court rejected the notion that an individual has no privacy interest in data that is publicly available somewhere. *See id.* at 770 ("In sum, the fact that an event is not wholly 'private' does not mean that an individual has no interests in limiting disclosure or dissemination of the information." (quotation omitted)). *See also* Reno v. Condon, 528 U.S. 141, 148 (2000) (upholding federal statute restricting states' sale of driver's license information to commercial entities even though the information was available to the public for a range of purposes).

commonly accepted "Fair Information Practices" captures this broader conception of privacy and is reflected, albeit in piecemeal fashion, in the various privacy laws and in the practices of commercial entities and government agencies. These principles govern not just the initial collection of data, but also the use of information collected and shared in the course of governmental and commercial transactions.

The "Fair Information Practices" were first articulated in the 1970s and have been embodied in varying degrees in the Privacy Act, the FCRA, and the other "sectoral" federal privacy laws that govern commercial uses of information. The concept of Fair Information Practices (FIPs) has remained remarkably relevant despite the dramatic changes in information technology that have occurred since they were first developed. While mapping these principles to the current data landscape poses challenges, and while some of the principles may be inapplicable to public record data, they provide a remarkably sound basis for analyzing the issues associated with creating a policy framework for the privacy of commercial databases.

The FIPs principles are variously enumerated, but we see eight: (1) notice to individuals of the collection of personally identifiable information, (2) limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, (3) limitations on the retention of data, (4) a requirement to ensure the accuracy, completeness and timeliness of information, (5) the right of individuals to access information about themselves, (6) the opportunity to correct information or to challenge decisions made on the basis of incorrect data, (7) appropriate security measures to protect the information against abuse or unauthorized disclosure, and (8) the

establishment of redress mechanisms for individuals wrongly and adversely affected by the use of personally identifiable information.[4]

A lot more work would be needed to develop a regulatory framework imposing all of these principles on all entities that hold or use personally identifiable data. Nevertheless, these principles do provide a framework for analyzing the current situation. They suggest certain immediate steps that Congress could take.

NOTICE OF BREACH

As a first step, there should be a national requirement that individuals be notified when their information held by a third party is obtained by an unauthorized user. CDT would support appropriate federal legislation modeled on the California disclosure law that would require holders of sensitive personal information to notify people whose information might have been stolen or otherwise obtained by unauthorized persons.[5] Some industry leaders have also supported federal notice legislation, as did the Chairman of the Federal Trade Commission at earlier congressional hearings.

The California law worked well after the ChoicePoint security breach. As a result of the California law, ChoicePoint was required to notify individuals so they could take protective action. And public pressure led ChoicePoint to give nationwide notice. California is currently the only state with such a law on the books, but other states are

---

[4] http://www.cdt.org/privacy/guide/basic/generic.html

[5] The California law states that any agency or business "that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.29(a), § 1798.82(a).

currently considering similar legislation. Congress should enact federal legislation that is as protective as the California statute.

There as been some debate about when entities should be required to give notice of a breach. Some have argued that the holder of the information should be allowed to exercise discretion in determining whether the breach is one that poses a significant risk of harm to individuals. Concern has been expressed that if consumers are notified of every security breach, they would receive too many notices and become immune to them. While the risk of over-notification is real, guidance issued by the State of California on its disclosure law seems to address concerns about over-notification. An appropriate standard might be to require entities that discover a breach of security of a system containing unencrypted personally identifiable data in electronic form to notify any U.S. resident whose data was, or is reasonably believed to have been, acquired by an unauthorized person. If the entity is not certain whether the breach warrants notification, it should be able to consult with the Federal Trade Commission. This would allow the entities to avoid giving notice in the case of accidental unauthorized access that does not pose a risk of harm to the public, while ensuring that the public is adequately protected in those cases where data has been acquired unlawfully. Additionally, it may be desirable to have a two-tiered system, with notice to the FTC of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. Broader notice to the FTC would help with oversight and would allow for adjustment in reporting thresholds.

Notice alone, however, is not enough. Consideration needs to be given to the question of what options a consumer has after receiving notice of a breach. Consumers can require a fraud alert on their credit reports, but under current law that has to be

renewed every 90 days unless the individual is actually the victim of identity theft, in which case he is entitled to a 7 year notice. Another approach is to give consumers the ability to "freeze" their credit reports, blocking their release and thus preventing the issuance of credit. Texas and California currently allow credit report freezes, and Vermont and Louisiana freeze legislation is supposed to take effect this summer. At least 15 other states are considering similar legislation.[6] Another way to allocate risk may be to create a "Do Not Issue Credit without Verification List," allowing consumers to post a warning to creditors to obtain additional identity verification before issuing credit. This would not be a freeze, but would put creditors on alert that they need to be careful.

SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

While notice legislation would be helpful in mitigating the damage from a security breach and might prod companies to improve security proactively, Congress should enact legislation requiring commercial entities that hold personal information to implement information security programs. Already there is a patchwork of requirements. Financial institutions are already subject to information security requirements under Gramm-Leach-Bliley,[7] and the Health Insurance Portability and Accountability Act imposes similar requirements on health care providers and insurers,[8] The Sarbanes-Oxley legislation also has a provision that is interpreted as imposing some kind of data security obligation. The Federal Trade Commission has exercised its Section 5 authority and

---

[6] Andrew Shain, "Nation, N.C. address ID security breaches," Charlotte Observer, Mar. 24, 2005, http://www.charlotte.com/mld/charlotte/11215774.htm.

[7] 15 U.S.C. § 6801(b).

[8] Pub. L. No. 104-191, § 264.

obtained consent agreements with a number of companies that are looked to as models. And the California law known as AB 1950 has imposed a general data security obligation on companies doing business there.

It is probably time to bring some uniformity to these requirements. The Federal Trade Commission regulations implementing Gramm-Leach-Bliley provide a good framework and probably have about the right level of detail for security programs for data brokers and other commercial entities.[9] They require an entity to develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards that are tailored to the size and nature of the entity. Among other elements of a security program, they require entities that hold personal information to conduct a risk assessment to identify and develop systems to protect against anticipated threats and unauthorized access to information, to train employees, to audit their systems to identify unauthorized access, and to periodically reassess the program's effectiveness. Otherwise, the FTC approach gives entities that collect and store personal information the flexibility to develop security programs that fit their business models.

SOCIAL SECURITY NUMBER PROTECTION

Personal privacy is not just threatened by ineffective or nonexistent information security systems, however. Another threat to personal privacy is the proliferation and misuse of Social Security numbers. When the federal government first issued Social Security numbers in 1936, it limited their use to identifying accounts for workers with earnings from jobs covered by the Social Security Act of 1935. Social Security numbers

---

[9] *See* Standards For Safeguarding Customer Information, 16 C.F.R. §§ 314.1-.5 (2005).

were not supposed to serve as the universal identifiers that they have become. In fact, they were initially called Social Security *Account* Numbers and for many years the words "Not For Identification" appeared on Social Security cards.[10] Over time, however, Social Security numbers have become de facto national identifiers, serving as the key that unlocks many databases containing medical records, university records, employee files and bank records, just to name a few.

Worse, the SSN is used as an authenticator. That is, it is used like a PIN number – even though SSNs are widely available, entities treat them as if they were a secret and that therefore someone is you if he knows your SSN. This is very poor security practice. As a result, Social Security numbers are a major factor in identity theft.

CDT supports legislation that would tighten controls on the sale, purchase and display of Social Security numbers. Given the ubiquity of Social Security numbers in the public domain, it might not be possible to prevent criminals from acquiring them, but that does not mean we should give up trying to curtail the SSN's overuse and misuse. We believe that this can be done without prohibiting the use of the SSN as an identifier or disambiguator in large databases. Certainly, the SSN should be phased out as a student or employee ID number reflected on ID cards, transcripts and other records disclosed outside an institution. Congress should also, where feasible, limit the use of Social Security numbers by government entities. In particular, states should be prohibited from using Social Security numbers on drivers' licenses.

These changes will have limited effect, however, unless it is also recognized that it is poor security practice to use the SSN as an authenticator – treating it like a password

---

[10] www.epic.org/privacy/hew1973report/c7.htm

or an obscure bit of information likely to be known only to the one person to whom it was issued. The habit of relying on the SSN for verification of identity needs to be broken.[11]

GOVERNMENT USE OF COMMERCIAL DATABASES

An often overlooked but very important issue is the federal government's use of commercial databases. As discussed earlier, the government uses commercial data for law enforcement and national security purposes. The Privacy Act of 1974 was supposed to subject government agencies that collect personally identifiable information to the Fair Information Practices, but the Act's protections only apply to federal "systems of records."[12] That means that the government can bypass the Privacy Act by accessing existing private sector databases, rather than collecting the information itself. Thus, although the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data.

---

[11] The habit of relying blindly on the SSN as an identifier also needs to be broken. See Lesley Mitchell, "New wrinkle in ID theft; Thieves pair your SS number with their name, buy with credit, never get caught; Social Security numbers a new tool for thieves," The Salt Lake Tribune, June 6, 2004, at E1.

[12] The term "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a).

Commercial information can and should play a key role in law enforcement and national security investigations. But agencies relying on that data should have clear guidelines for its use—guidelines that both protect individual rights and ensure the information is useful for investigative purposes.

One option would be to make it clear that the Privacy Act applies whether the government is creating its own database or acquiring access to a database from a commercial entity. Also, Congress could apply the concept of Privacy Impact Assessments to the acquisition of commercial databases. Section 208 of the E-Government Act of 2002 already requires a PIA if the government initiates a new "collection" of information.[13] The same process should apply when the government acquires access to a commercial database containing the same type of information that would be covered if the government itself were collecting it.

Another approach, based on a bill that Senator Wyden introduced in the last Congress,[14] would be to require the government to perform an accounting of private sector databases before using them. Under the Wyden proposal, a government agency that acquired access to databases containing personally identifiable information

---

[13] E-Government Act of 1002, Pub. L. No. 107-347, § 208(b)(1). Under the E-Government Act, an agency is required to perform a privacy impact assessment before it "develop[s] or procure[s] information technology that collects, maintains, or disseminates information that is in an identifiable form" or "initiat[es] a new collection of information...." § 208(b)(1)(A). A privacy impact assessment is required to address, "(I) what information is collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; (VI) how the information will be secured; and (VII) whether a system of records is being created under" the Privacy Act. § 208(b)(2)(B).

[14] S. 1484, 108th Cong. (1st Sess. 2003).

concerning U.S. citizens would be required to publish in the Federal Register a description of the database, the name of the entity from which the agency obtained the database and the amount of the contract for use of the database. In addition, the agency would be required to adopt regulations that establish

- the personnel permitted to access, analyze or otherwise use the database;
- standards that govern the access to and analysis and use of such information;
- standards to ensure that personal information accessed, analyzed and used is the minimum necessary to accomplish the government's goals;
- standards to limit the retention and re-disclosure of information obtained from the database;
- procedures to ensure that such data is accurate, relevant, complete and timely;
- auditing and security measures to protect against unauthorized access to or analysis, use or modification of data in the database;
- applicable mechanisms that individuals may use to secure timely redress for any adverse consequences wrongly experienced due to the access, analysis or use of such database;
- mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies or guidelines; and
- an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or unauthorized access to or use of the database.

Agencies might also incorporate into their contract with commercial entities provisions that provide for penalties when the commercial entity sells information to the agency that

the commercial entity knows or should know is inaccurate or when the commercial entity fails to inform the agency of corrections or changes to data in the database.

The Intelligence Reform Act that Congress passed last December established guidelines for the government's evaluation of Secure Flight plans that suggest a broader framework for use of data.[15] Congress could adopt similar guidelines for government agencies to follow before implementing any screening program that uses commercially available data. As an initial matter, all government screening programs should be congressionally authorized. This would ensure some degree of public accountability and congressional oversight. In addition, all screening programs should be subject to regulations that include, at a minimum, the following elements:

- procedures to enable individuals, who suffer an adverse consequence because the system determined that they might pose a security threat, to appeal the determination and correct any inaccurate data;
- procedures to ensure that the databases the government uses to establish the identity of individuals or otherwise make assessments about individuals will not produce a large number of false positives or unjustified adverse consequences;
- procedures to ensure that the search tools that the department or agency will use are accurate and effective and will allow the department or agency to make an accurate prediction of who may pose a security threat;[16]
- sufficient operational safeguards to reduce the chance for abuse of the system;

---

[15] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012(a).

[16] This provision is drawn from the Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, § 552.

- substantial security measures to protect the system against unauthorized access;
- policies that establish effective oversight of the use and operation of the system; and
- procedures to ensure that the technological architecture of the system does not pose any privacy concerns.

These approaches, all of which Congress has previously approved in similar contexts, strike a balance between the government's need for information and the privacy interests of individuals. Adapting the Privacy Act and Fair Information Principles to government uses of commercial databases would go a long way toward closing the unintended gap in privacy protection that exists under the current law.

REGULATION OF DATA BROKERS

Finally, Congress should consider whether there are gaps in the current sectoral laws that protect privacy and focus on the harms that can flow from use of inaccurate or misleading information. This is not about use of marketing data to send catalogues or sales offers. Rather, in the context where adverse consequences can result, Congress should apply to data brokers the Fair Information Practices that are the framework of the Fair Credit Reporting Act and other privacy laws.

As the law stands now, these Fair Information Practices apply only when data brokers collect and use information in a way that is governed by the Fair Credit Reporting Act. For instance, if a data broker sells personal information to a third party that uses the information to determine eligibility for insurance, the Fair Credit Reporting Act would apply and certain rights would attach to the individual to whom the information pertains. The individual would be able to obtain a copy of the report,

challenge the accuracy of the data and correct any inaccurate information. The ability to do this is particularly important when a person can suffer adverse consequences—such as the denial of insurance—from the use of the personal information. But if the data broker sold that same information to an insurance company for use in claims processing – in which case the individual might be denied reimbursement under her insurance policy - the individual would not have any of those same rights.[17]

We note that Derek Smith, the Chairman and CEO of ChoicePoint, last year called for a national dialogue on privacy, to develop a policy framework for his companies and others. Specifically, Smith called for expanding the principles reflected in the FCRA:

> "We should agree that the consensual model is best to the maximum degree possible, understanding that law enforcement and national security uses may outweigh getting prior consent for certain information. By this I mean that individuals should give permission (or not) at the time information is gathered and should agree to its use. Data should not be used for a different purpose unless new permission is obtained. However, we must recognize that public record data is, fundamentally, just that – public – and does not fit within the consensual model because of the current local, state, and federal freedom of information acts.
>
> Everyone should have a right of access to data that is used to make decisions about them – subject to the same caveats about law enforcement and national security uses. In other words, expand the principles of the Fair Credit Reporting Act to all types of information: right to access, right to question the accuracy and prompt a review, and right to comment if a negative record is found to be accurate."[18]

---

[17] Michael Hiltzik, *Data Show Information Collector Can't Be Trusted*, Los Angeles Times, Mar. 3, 2005, at C1.

[18] Derek V. Smith, "Risk Revolution: The Threats Facing America and Technology's Promise for a Safer Tomorrow" (Longstreet Press, 2004) 185.

CONCLUSION

Resolving these issues will require a broad-based and inclusive dialogue. We must strike a balance, but the current absence of a comprehensive legal framework for the collection, sale and use of sensitive personal information is yielding harms that are made clear every day. The Center for Democracy and Technology looks forward to working with the Committee, with all of today's witnesses, and with all stakeholders. We are not helpless in the face of the ongoing revolution in information technology. Through the policy process, we can decide whether there is "No Place to Hide."

Testimony of Robert Douglas
CEO, PrivacyToday.com
Before the
United State Senate Committee on the Judiciary
--
Hearing on
Securing Electronic Personal Data: Striking a Balance
Between Privacy and Commercial and Governmental Use
--
April 13, 2005

My name is Robert Douglas[1] and I am the CEO and founder of PrivacyToday.com located in Steamboat Springs, Colorado. I provide consultation to the private and public sectors on issues involving all aspects of identity theft, identity fraud, and personal information security. During the past eight years my work has centered on assisting the financial services industry, the general business community, government, and law enforcement agencies to better understand the scope and methodology of identity crimes through educational materials, presentations, auditing, and consultation.

I have provided consultation and expert testimony for civil and criminal investigations brought by private parties and state and federal law enforcement agencies. Most relevant to today's hearing, I served as a consultant and expert witness for the Federal Trade Commission in the design and execution of Operation Detect Pretext, a sting operation to catch and civilly prosecute individual and corporate offenders participating in the illegal "information broker" industry.[2] I served as an expert witness to the Florida Statewide Grand Jury on Identity Theft. I served as an expert witness and consultant for the plaintiffs in a federal civil action brought by the parents of Amy Boyer, a young woman slain in a murder committed by a man who purchased Ms. Boyer's social security number, date of birth, and place of employment from a web-based information broker.[3] I have lectured before local, state, federal and international law enforcement associations on the topic of identity crimes. I have been a private investigator and security consultant for the past twenty-two years. This is my fifth appearance before the United States Congress to discuss personal information security.[4]

The Murder of Amy Boyer

Far too often as we grapple with the issue of balancing the privacy of Americans with the necessary and legitimate uses of Americans' personal information the debate centers on

---

[1] Resume of Robert Douglas is located at Appendix I.
[2] See http://www.ftc.gov/opa/2001/04/pretext.htm for the FTC's Operation Detect Pretext web page.
[3] See Appendix II: Remsburg v. Docusearch, The Supreme Court of New Hampshire.
[4] See Appendix III & IV for testimonies relevant to today's hearing: July 28, 1998 Hearing on "The Use of Deceptive Practices To Gain Access To Personal Financial Information" (U.S. House of Representatives Committee on Banking and Financial Services) and September 13, 2000 Hearing on "Identity Theft and Related Financial Privacy Issues" (U.S. House of Representatives Committee on Banking and Financial Services).

discussions of "data", but not the lives behind the "data". In order to illustrate what I've learned over the course of more than twenty years using and investigating the good and harm of database information, I'd like to begin by focusing on one life behind one set of data. The untimely and violent end to that life encapsulates all the issues that surround securing personal information while balancing privacy with legitimate uses of information. Further, investigating this one act of violence led me to a more complete understanding of how personal information is being used and abused in the United States today. This case also demonstrates that the problem is much larger than the recent ChoicePoint breach and other instances that have recently been in the headlines. The problems of securing personal information and balancing privacy with legitimate use are intertwined and impact every business and government sector.

On a quiet fall afternoon in October of 1999 Amy Boyer, a young Nashua, New Hampshire woman, was leaving work with two co-workers. The small group was discussing plans for that weekend as they walked to their cars parked on a side street less than a block from the office. As Amy said good-bye and closed her door, a car driven by Liam Youens sped up the street and stopped driver's door to driver's door with Amy's car. Youens yelled out Amy's name as he fired 11 bullets into the head and upper body of his unsuspecting 20 year-old victim. Youens then fired one last shot into his head, instantly killing himself as Amy lay just feet away mortally wounded.

Liam Youens was a demented young man. He glorified the Columbine killers and toyed with the idea of doing the same at Nashua High School. He openly planned Amy's murder and the intended murder of others for more than a year. The reason we know so much about Youens is that he documented his plans to murder Amy on a web site he created to publish his sick desires.

But that web site contained far more than just the perversity of Liam Youens. It contained the starting point for a trail of evidence that proves how personal information of all Americans stored with good intent in myriad databases across this country can be easily obtained and used for incalculable harm. The trail that began on a quiet Nashua street led to the shadowy world where a small but persistent number of illegitimate information brokers and private investigators, in addition to a growing number of identity thieves and other criminals, access databases holding our most important personal information and use that data for criminal purposes.

In Amy's murder the evidence showed that Youens decided to ambush Amy as she left work. But Youens had a problem. He didn't know where Amy worked. So he started using information brokers and private investigators that run Internet based operations that specialize in obtaining and selling personal information on Americans. In separate Internet transactions Youens purchased Amy's date of birth, social security number, home address, and finally her place of employment.[5]

[5] For a more complete recitation of the facts surrounding Youens' purchase of Ms. Boyer's information see The Supreme Court of New Hampshire opinion attached as Appendix II.

Youens himself was struck by how easily he was able to purchase Amy's personal information while concealing his evil intent. Here is a small sampling of Youens own words from his web site where he was documenting his step-by-step activities to locate and kill Amy:

> *When I finished finding* [street name redacted] *residents in the phone book I thought my best bet was apt. number 7 so I entered the information. It wasn't 7, but who cares I got a HIT! I fell to the floor and let the endorphines fly. Her address was* [residential address redacted] *she didn't move from home yet, no other information was provided in the background check.*
>
> *I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment.* ***It's accually obsene what you can find out about a person on the internet. I'm waiting for the results.***
> [typos from original/redaction and emphasis added by R. Douglas]

The Internet site Youens found to get Amy's "current employment" and "everything else under the Sun" was Docusearch.com. To obtain Amy's "current employment" Docusearch provided Amy's social security number, date of birth, and home address to Michele Gambino, another private investigator/information broker operating as Gambino Information Services out of New York City. Gambino has at times described her specialty as "proper pretext", "subterfuge phone calls", or "informative telephone conversations". Those are nice titles for deceit, fraud, and lying. In short, Gambino uses lies to deceive people out of personal information.

At the time of Amy's murder, Gambino and others who worked as subcontractors for Docusearch specialized in defeating the information security systems of financial institutions (including many of the nation's largest banks and brokerage houses), telecommunications companies (obtaining non-published phone numbers and records of phone numbers dialed from any phone in the country), utility companies (power/cable/gas/water/satellite firms all maintain databases of personal information), and unsuspecting private citizens with information about loved ones.

In this case, Gambino conducted a "pretext" to obtain Amy's work address by impersonating an insurance company representative and falsely stating that she had a refund for Amy. By having Amy's social security number, date of birth, and home address, Gambino was able to sound authoritative as most Americans wrongly believe that only someone with legitimate access and authority would have their social security number and other personal information. Gambino was able to deceive Amy and/or Amy's mother out of Amy's work address on the pretext that the work address was needed to process the insurance refund.

The reality is, as far as Docusearch and Gambino were concerned, obtaining Amy's work address by fraud was just another transaction to put money in their pockets. And a lucrative business it is. With just two employees and a handful of independent

contractors like Gambino, Docusearch was grossed over $1 Million per year selling and re-selling Americans' personal information.[6]

Outrageously, while Docusearch was in the business of accessing and stealing Americans' personal information and continues to this day to brag about how they can find anything about anybody, neither Gambino nor Docusearch took any constructive steps to determine who Youens was, much less why he needed the employment address of Amy. Had Docusearch or Gambino simply typed Amy's name into any free search engine they would have found Youens' web site documenting his intent to kill Amy.

Docusearch was on notice that their Internet site was being used by potential stalkers with intent to do harm. Just days before Gambino used a "pretext" to obtain Amy's work address, Docusearch learned that another "client" was attempting to obtain an address on a young woman in Texas for potential harm. In the Texas case, Docusearch was once again using a pretext to learn the address of the young woman from the woman's mother. Fortunately, the mother was savvy enough to realize they were trying to deceive her out of her daughter's address and told the Docusearch "investigator" that her daughter had a restraining order against Docusearch's client.

While Docusearch, Gambino, and others in the information brokerage and investigative fields often argue that they shouldn't be held responsible for the unforeseen consequences of selling "data", those defenses ring hollow. Not only is there ample evidence in the files of Docusearch and Gambino of potential harm caused by the personal information they are selling on demand, the information brokerage/private investigative industries have been aware since at least the early 1980s of criminals using their services to carry out violent and non-violent crimes.

Congress Passed the DPPA and Other Statutes to Protect Americans

In March of 1982 the information broker/private investigative professions and all who maintain databases with personal information learned first-hand that personal information in the wrong hands can lead to severe physical harm or murder. In a scenario frighteningly similar to what happened to Amy, actress Theresa Saldana was repeatedly stabbed and slashed by a stalker at the front door of her home. To find Saldana, the stalker hired a private investigator to obtain Saldana's mother's non-published phone number. The stalker then called Saldana's mother and tricked her into providing Saldana's home address by using the "pretext" that he was Martin Scorcese's assistant and needed Saldana's home address in order to reach Saldana for a movie role.

[6] It is ironic given the circumstances of today's hearing and the tangled if tangential relationship between Docusearch and ChoicePoint that Forbes Magazine lists Docusearch first and ChoicePoint second on the Forbes.com Best of the Web for Investigators Tools. But even Forbes in the description for the category states: "The sites below can help you in your digging. Of course, the flipside is that scam artists and snoops can easily obtain private information on you." Perhaps Forbes should add murderers to the list after scam artists and snoops.

Following the Saldana attack, came the 1989 murder of actress Rebecca Schaeffer. In that case, a private investigator obtained Schaeffer's home address through the California motor vehicle database and sold the address to a stalker. The stalker used the address information to stalk and kill Schaeffer. The attack of Saldana and the murder of Schaeffer, combined with a growing body of evidence that personal information contained in state motor vehicle records (at that time routinely provided to anyone requesting it) was being used for criminal purposes, led to passage of the Drivers Privacy Protection Act (DPPA). A federal law that I would argue is violated thousands of times each day.[7]

But the trail of evidence in Amy's murder does not end with an obsessed killer and a couple of greedy private investigators operating Internet information brokerages. Quite simply, the evidence in Amy's murder leads to thousands of documents demonstrating in real time how databases maintained in a wide range of American businesses and entire industries that contain our most personal information are breached everyday.

Commercial/Government Information Security Systems Are Breached Every Day

On a daily basis Docusearch, Gambino, and other associates of Docusearch were penetrating the information security systems of this nation's financial services industry, postal service, telecommunication and other utility companies, and selling that personal information to just about anyone. Contained within the files of Docusearch, Gambino, and hundreds of other similar companies is evidence that not only can any piece of information about anybody or any company be obtained by anyone willing to pay for it, but clear and convincing evidence that when it comes to being guardians of critical personal information both government and commercial entities deserve a failing grade.

Unfortunately, Docusearch and Gambino are not rare examples that limit the scope of the problem to a finite few. The reality is there are hundreds of "Docusearchs" combined with thousands of identity thieves conducting arguably tens of thousands of breaches of information security systems across all business and government sectors each day in this country. You don't get ten million identity theft victims and fifty-plus billion dollars in losses to identity theft related financial fraud from dumpster divers.

To further illustrate the scope of the problem, consider what we already know when it comes to the black market of personal information provided by unscrupulous information brokers and private investigators. Remember, these unscrupulous companies are a window into the very same methods used by criminals, identity thieves, and potentially terrorists.

[7] There are dozens of web sites selling DPPA protected driver's information. While many of these sites quote the language of DPPA the reality is, just like purchasing social security numbers, anyone can purchase federally restricted driver's information.

Federal Trade Commission's Operation Detect Pretext

Following my second of two appearance before the House Banking Committee[8], in which I assisted the Committee with a surreptitious survey of online Internet information brokers and their offerings that confirmed financial information of Americans was for sale, I worked with the Federal Trade Commission to design a sting operation to civilly prosecute Internet based information brokers selling financial account information (including specific account numbers and balances) in violation of the Gramm-Leach-Bliley Act. Operation Detect Pretext, as it was named, revealed that there were hundreds of Internet based information brokers and private investigators advertising the sale of Americans' most personal information in violation of any of a number of federal statutes including but not limited to Gramm-Leach-Bliley, the FCRA, the DPPA, and the Unfair and Deceptive Trade Practices Act. There was also evidence in the files of at least one of the FTC targeted information brokers of the broker selling personal information (perhaps unknowingly) to identity thieves.[9]

The reality of how the Docusearchs, Gambinos, and identity thieves (as we know from the recent ChoicePoint case) defeat the information security systems of so many companies is that they often begin by acquiring the personal information of the victim of the intended crime. Using this personal information the criminal or unscrupulous information broker can impersonate the victim in order to obtain further personal information or carryout a criminal act by convincing the rightful custodian of personal information to reveal it to the criminal posing as the victim.

As an information broker once explained the process to me:

1) Know what piece of data you want.
2) Know who the custodian of the data is.
3) Know who the custodian will release the data to.
4) Know what circumstances are needed for the release of the data.
5) Become (impersonate) that person with those circumstances.

Illegitimate Subscriber Access – The Resale Market

Unfortunately, many of the illicit information brokers who will steal and sell any information about anybody have subscriber access (through a variety of legitimate and illegitimate means) to the legitimate information brokerage companies. They need the biographical information contained in the databases of the legitimate information brokers in order to carry out their pretexts like Gambino did to Amy. Specifically, to carry out the 5 steps outlined above, the unscrupulous information broker, private investigator or identity fraud criminal will purchase the biographical data needed (from either a legitimate information broker via a fraudulent subscriber agreement as in the instant ChoicePoint case, or via a reseller who obtains the information from a legitimate broker and willingly violates the no resale contract) in order to impersonate an individual that desired information will be released to.

---

[8] See Appendixes III & IV.

[9] See http://www.ftc.gov/opa/2001/04/pretext.htm for the FTC's Operation Detect Pretext web page.

There are a number of information brokerage companies, in addition to ChoicePoint, that have maintained relationships with information brokers and private investigators that I classify as resellers. While ChoicePoint and several other brokers have announced they will further restrict access to full social security numbers, dates of birth, and other personal identifiers to some clients of certain size and business lines, there is no doubt that absent legislation other companies will step in to fill the void—even if the ChoicePoint-styled self-remedy is effective. The hottest topic in the private investigative and information brokerage fields right now is where can you obtain full social security numbers and from what companies. The information resellers and investigative markets will flock from ChoicePoint to other mainstream information brokers willing to accept the revenue until Congress acts.

Indeed, for many years information resellers have easily deceived the major information brokers in the application process or violated the no resale clauses of their contracts. This is the worst kept secret in the information broker/investigative world.

Information Security in the U.S. is Laughable at Best

But even if all legitimate information brokers were to appropriately and effectively secure the data in their electronic warehouses, the flow of information would continue. Criminals and others will just access, and in many cases continue to access, databases from the government and private sector to find the personal information they need for their crimes.

When it comes to the overwhelming majority of databases in this country from government maintained military, postal, education, tax, welfare, and child support records to commercially maintained financial account, telecommunications, utility, medical, and business records, the information can almost always be obtained by an individual named in the records. Often this is the actual account holder. For the unscrupulous information broker or criminal, it is merely a matter of piecing together enough personal information about the targeted victim to impersonate the victim to the custodian of the information. And with far too much frequency, the key to unlocking most personal information is the social security number.

As I demonstrated a week ago in a story by Jonathan Krim of the Washington Post, it is a simple matter to go on the Internet and purchase from any one of a number of information brokers the social security number of any American. But even if social security numbers were not easily obtained from information brokers through direct or indirect (the illicit resale market), the indisputable fact is social security numbers have been compromised in this country in many ways for such a long period that it is laughable that either government or commercial enterprises use the number as a personal identifier for maintaining security of databases.

Yet this is the method chosen by more than 50% of the nation's banks, telecommunication companies, hospitals, doctor's offices, universities, utility providers,

government programs, and almost any government or commercial entity one can name. I can inform this Committee and easily prove to this Committee based upon my experience investigating and studying information security practices and criminal methods for defeating those practices, and from the documents available in the Boyer murder case (that I would gladly share with this Committee in a closed setting), that any information security system using personal biographical information as the primary security identifier to allow access to the information is a fatally flawed system.

Congress Should Outlaw the Use of Personal or Biographical Identifiers for Information Access

Let me blunt. If this Committee and this Congress want to take a giant step down the road to securing Americans' data stored across all government and commercial entities, that step should be to prohibit the use of social security numbers, dates of birth, addresses, phone numbers, mothers maiden name, and any other personal biographical identifiers as information access security protocols. The reason for prohibiting the use of personal biographical information as security protocols for access to information maintained in databases is simple. Anyone can find them for free or buy them in hundreds of locations and databases across the country and on the Internet.

Why is it critical that we maintain the security of these databases? Because the vast majority of personal information contained in databases across this country is used for purposes that benefit Americans every day. Those benefits include commercial applications that assist citizens in transactions that weren't possible even ten years ago, but that we now take for granted. Additionally, the personal and biographical data maintained in a wide range of storage methods can be of critical value for government in fulfilling constitutionally mandated societal welfare, law enforcement, military, and national security functions. In the commercial sector personal information databases can assist in expediting transactions resulting in lower costs in addition to fraud prevention, detection, and prosecution.

The challenge is to determine a way to maintain this information which can be used for good and harm in a secure way that guarantees it is available for good, but not harm. As with any challenge, we must first understand the scope of the problem.

As I've tried to demonstrate through the evidence uncovered in the Boyer murder case, the scope of the problem far exceeds the ChoicePoints of the world. I am not here to make excuses for ChoicePoint or the other "legitimate" information brokers who after all do provide critical information to government and the private sector as discussed above.[10]

[10] In the interest of full disclosure, for a brief period I worked as an independent contractor for ChoicePoint on matters dealing with potentially fraudulent subscriber agreements.

In fact, I think the most recent breach that was the catalyst for this hearing is inexcusable given ChoicePoint's prior knowledge of attempts to fraudulently obtain subscriber access.[11]

Legislation Must Address All Commercial and Government Entities

Yet to limit any proposed legislation to the information broker industry would be short-sighted in my opinion. After all, information brokers are nothing but aggregators of data contained in a wide variety of storage media. From courthouses; state, local, and federal offices; and, the military to marketing lists; phone directories; credit bureaus; insurance companies; and, dozens of commercial industries, information brokers gather "data" that is re-packaged and sold for a wide variety of uses.

If Congress takes action that only affects the commercial information broker industry while ignoring the government and the private business sector databases where information brokers obtain their raw data, there will be little accomplished. This is because criminals and others who would use information for illegal purposes will turn to the original sources of that raw information.

To place the question as to scope of the problem and how to curb it in the framework of the recent ChoicePoint breach, ask the following question: What good is to mandate that ChoicePoint have adequate security protocols to protect our personal information if the banks, telecommunication companies, universities, hospitals, doctors offices, insurance companies, utility providers, car dealers, and governmental agencies don't have adequate security protocols and are as porous when it comes to information security as ChoicePoint was?

If the ChoicePoint debacle causes this Committee and Congress to begin to seriously re-think how we protect all forms of data in this country, particularly at a time of war when our enemies have proven adept at understanding and using to their advantage information systems (such as deficiencies in driver's license cross-reference verification systems that allowed issuance of multiple driver's licenses from multiple jurisdictions to the 19 September 11th hijackers) then a complete understanding will be needed of how information too easily accessed and used for harm can be secured across the board and used for the benefit of individuals and the security of the nation.

---

[11] The immediate case where a Los Angeles based group stole the data of 145,000 Americans is not the first time ChoicePoint has learned of problems in its subscriber verification process. ChoicePoint has been aware since at least the time of Ms. Boyer's murder in 1999 that an indeterminate number of subscribers and those attempting to subscribe to the company were falsifying applications in order to gain access to ChoicePoint databases. In fact, ChoicePoint notified Ms. Boyer's parents' legal team that they had caught Docusearch trying to obtain a subscriber agreement with ChoicePoint under false pretenses even after Ms. Boyer's murder and a suit being brought against Docusearch. But ChoicePoint is not alone in this knowledge. It has long been understood amongst the major credit bureaus and information brokers that smaller information brokers and private investigators were reselling information products in violation of subscriber agreements.

But it must be a holistic approach. There are far too many sources of personal information in this country to either believe we can put the genie back in the bottle when it comes to social security numbers and other personal biographical identifiers or that we can solve the problem of securing information by addressing industries on a piecemeal basis.

In fact, Congress has tried the piecemeal approach for years with different issues, governmental agencies, and commercial industries. From the Privacy Act (restrictions on government use of personal information) to the Fair Credit Reporting Act (restrictions on consumer reporting agencies use of personal information) to the Driver's Privacy Protection Act (restrictions on state motor vehicle agencies handling of personal information) to most recently Gramm-Leach-Bliley (restrictions on financial institutions use and handling of personal information) Congress has addressed issues of privacy, data protection and data access on a case by case basis.

I would urge this body to recognize and accept as fact that many of the same challenges when it comes to securing personal data while balancing the legitimate privacy of Americans with the legitimate needs of government and beneficial commercial practices permeate all aspects of American government and private business. It is time to mandate that all government entities and the business community develop practical and effective information security programs that address 1) appropriate use questions (who gets access) and 2) authentication issues (how access is granted in a secure method).

If we don't take this approach across all sectors, criminals and this nation's enemies will do just as the unscrupulous and illegitimate information brokers I've discussed throughout this testimony do should they be effectively cut off from access in one database. They'll just turn to the next database in the next industry that has not been protected.

Need For A GAO Investigation

I have seen a number of investigations done by the GAO which provide a blueprint for an investigation this Committee might find beneficial as it grapples with the issues at hand. The two most relevant investigations were: 1) An investigation as to how easily undercover GAO investigators using movie prop badges and fake law enforcement IDs created with off the shelf software were able to access secure government facilities and secured areas of airports; and, 2) An investigation as to how easily undercover GAO investigators were able to obtain state issued driver's licenses by submitting obviously fraudulent identity documents to counter clerks.

Perhaps this Committee would consider requesting the GAO to perform an investigation of how easily they can access telecommunication company databases; financial services companies databases; utility companies databases; hospital databases; university databases; and, state and federal government agency databases, all by means of social engineering/pretext. I think the results would be enlightening.

Oversight and Enforcement Are Critical

Additionally, Congress needs to exercise oversight on the agencies already charged with enforcing the FCRA, GLBA, DPPA, and other applicable privacy and data security laws. From credit reports, to financial account information, to driver's records and beyond—it is all for sale by hundreds of companies routinely laughing in the face of Congress and the laws that are not enforced.

Those laws were passed with reasons that were important at the time, but are even more important in the age of terrorism that has been visited upon our shores. Our porous information systems in this country are a terrorists dream and a potential terrorist tool.[12] It is time we get serious about protecting information of all forms in this nation.

In addition to the dangers of criminals, terrorists, identity thieves, and illicit information brokers who violate Americans' privacy there is an equally compelling reason to take action to protect personal information. The very same information that is too often abused is the life blood of this country and all Americans. If Americans don't have faith that the information they provide is secure it will harm commerce, and more fundamentally, the trust we all place in those that we share our most important and private data with.

In closing, I'd like to make an offer to this Committee, any other Committee of the Congress, any individual Senator of Representative, or any agency of the United States government. I will gladly volunteer my time and resources, including the information and evidence I've gathered over the last 8 years, to provide as much assistance as I can to securing the personal information of Americans.

Thank you.

[12] After my first testimony on information brokers in July of 1998, I was asked by Pentagon representatives to demonstrate how the data and techniques used and obtained by information brokers could be used to harm the military at a time of "force protection". With out revealing what I showed the Pentagon representatives in this open forum, I can state that the starting point was a background search of the type offered by ChoicePoint and other information brokers.

Welcome to www.Secret-Info.com

LOCATE SEARCHES:
* Trace A Social Security Number
* Locate A Social Security Number
* Mini Skip Profile Packs
* Super Skip Profile Packs

PHONE SEARCHES:
* Reverse Phone Number Trace
* Unlisted Reverse Phone Trace
* Telephone Number Locate
* Unlisted Phone Number Locate
* Land Line Telephone Tolls
* Cellular Phone Tolls

VEHICLE SEARCHES:
* License Plate Traces
* VIN Traces
* Drivers License Numbers

ASSET SEARCHES:
* Watercraft Ownership Information
* Aircraft Ownership Information
* Property Ownership Information
* Pilots License Information

Billions of Public Records Now Available to You!

Arm Yourself With The Facts!

Call & Talk Live One-On-One With Our Private Investigator!

1.704.888.6090 9am - 8pm Mon-Fri Eastern Standard Time

*** Trace A Social Security Number**
You supply a social security number and we supply you with the name and most current address!

*** Locate A Social Security Number**
Supply a name & address or previous address, we will supply a social security number!

*** Mini Skip Profile Packs**
You supply a social security number, we supply a small profile report on the subject, such as name, akas, date of birth, phone number, neighbor information, possible driver license number and more!

*** Super Skip Profile Packs**
You supply what ever you have! we supply a large detailed profile report on a subject, including name, date of birth, AKA's, address history, relatives, property ownership, business ownership, phone number, neighbor information, vehicle information, licenses, aircraft and boat ownership and much more! Information returned varies state to state.

SLIDE 1

Locate A Social Security Number :

Supply a name & address or previous address, we will supply a social security number !

For Accurate Results, Provide As Much Information Below as Possible:

Locate A Social Security Number - MBL	Search Order Code
	Full Name To Be Searched
	Social Security Number
	Date Of Birth
	Current Address
	City, State, Zip
	Previous Address
	Tag / Plate, State
	Current Phone Number
	Previous Phone Number
	Drivers License Number
	AKA's
	Employment

Detailed Description :

Customer Information :

"IMPORTANT NOTICE" For Your Protection, We Will Contact You To Verify That You Have Requested The Search. A Valid Phone Number Where You Can Be Reached Is Required. A Search Will Not Be Performed Until We Have Contacted You.

	Your Full Name (Required)
	Your Company Name
	Your E-Mail Address (Required)
	Your Street Address (Required)
	Your City, State, Zip (Required)
USA	Your Country
	Your Home Phone Number (Required)
	Your Work Phone Number (Required)
	Your Fax Number

SLIDE 2

Term & Conditions :

I understand that I am placing an order or orders for a search on an electronic or mechanical database through a fallible source, and assume full responsibility for inaccurate or incomplete identifying information submitted or results received. I agree that MYTOYO Inc. is held harmless for errors omissions, and cannot guarantee the accuracy or completeness of reports for the fee or fees charged. I understand that requests may **not** be canceled & understand payment is still due **hit** or **no hit**. I certify that all requests are submitted in accordance with the FCRA 91-509 and all other laws that may apply.

I hereby swear that I will be personally liable for any and all charges made by the above named company . I understand that if any of these debts are not paid in full within Thirty (30) days from the invoice date that these debts may appear on my personal credit rating as well as that of the company. I ALSO AGREE THAT BY SIGNING BELOW I AM AUTHORIZING THE CHARGE/DEBIT INDICATED ABOVE AND THAT THIS WILL BE MY METHOD OF PAYMENT FOR FUTURE ORDERS UNLESS AGREED DIFFERENTLY IN WRITING IN THE FUTURE. I ALSO AGREE PAYMENT IS DUE HIT OR NO HIT OF INFORMATION. I further attest that I understand the Fair Credit Reporting Act (15v.s.c.1681) and certify that requests will only be made for the following reasons listed below and no other: "Permissible purposes of reports:"

A consumer reporting agency may furnish a consumer report under the following circumstances and no other:
To a person which it has reason to believe - (A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or (B) intends to use the information for employment purposes; or (C) intends to use the information in connection with the underwriting of insurance involving the consumer; or (D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status.

I also attest that all information obtained from MYTOYO Inc. will be used for lawful purposes and hold MYTOYO Inc. and/or Secret-Info.Com suppliers harmless in any actions arising from use or misuse or reliance on the information supplied. I understand that the fees are for searches, not the actual information and that while MYTOYO Inc., strives to obtain valid information, there are no warranties, express or implied, of information returned.

Select Your Payment Method : Visa, MasterCard, Discover or Check

My preferred payment method will be:

☐ ☒ **Cash or Money Order Click Here!**

☐ **$35.00 Visa, MasterCard, Discover or Check Using This Form**

Note: If you are paying by check, type in all fields excluding the credit card information, print this form, make out and send payment to: **North American General · PO Box 385 · Locust, NC 28097**

Visa - $35

Card Expiration Date (Required)

Card Number (Required)

Name of Card Holder (Required)

A 10% Discount Is Issued For Multiple Searches Within 30 Days

Submissions Without Payment Information Are Discarded

I Have Read And Accept The Terms & Conditions Above :

I Agree | Clear

PHONE: 1.704.888.6090 9am - 8pm EST
FAX: 1.704.888.1849

North American General
Address: P.O. Box 385
Locust, North Carolina 28097

SLIDE 2

From: Michael
Date: Wednesday, March 30, 2005 9:27 AM
To: [email address redacted]
Subject: search results

Dear Robert
The following are your search results.
As agreed your credit card has been charged $ 35.00
and will appear on your next credit card statement as
Mytoyo Inc or Mytoyo Inc investigative services
authorization: [auth# redacted]
You should receive your receipt in the mail in the next few days.
If you have any questions please give me a call 704-[phone# redacted]
Thanks again

Michael
http://www.secret-info.com

Jonathan Krim XXX-XX-XXXX [SSN redacted]

iinfo .com

Find someone fast with the People Search Company. Obtain phone reports, background checks and locate missing people. We're dedicated to helping repossession companies, investigators, attorneys, paralegals, and business professionals find people, phone numbers and address data they need.

See what our customers say about our people search services.

The People Search Company ™

- About Us
- Directory
- Refund Policy
- How to Order
- Contact Information
- Free Searches
- Resource Guide
- F.A.Q.'s
- Link Exchange
- Terms & Conditions

Send Me Tips, Secrets & Spy Info!
E-Mail Address:

Can you receive HTML e-mail? Yes
Subscribe

Best Spyware Removal Software

3 BUREAU Credit Reports

Select a specific people search service, or specific category listed below. People Search category lists contain a summary of each people search. Click here to view a complete directory of all people search services.

Name & Address Search Directory
- Basic People Locator Search
- Super Exhaustive Background Check
- Name & address from Unlisted Phone
- Name & address from Pager or Voice mail
- Name & address from Disconnected Phone
- Name & address from Toll Free or Pay Phone
- Name & address from Cellular phone number
- Name & address from Disconnected Cell

Toll Call Search Directory
- Residential Local Toll Call Report
- Residential LD Toll Call Report
- Business LD Toll Call Report
- Cellular Phone Toll Call Report
- Cell phone name, address & call report

SSN Search Directory
- Social Security Number (SSN) Tracer
- Social Security Number (SSN) Finder

Post Office Search Directory
- Search for address from P.O. Box number
- Search for address from Personal Mail Box

Cell Phone Search Directory
- Find name & address from cellular number
- Name & address from disconnected cell
- Search for someone's cell phone number
- Cell Phone Call Records Report
- Find name, address and cell phone records from any cell phone number

Utility & Reverse Search Directory
- Name & unlisted phone number from address
- Utility Search - find unlisted phone number & address from Name, SSN & City

DMV Search Directory
- Search VIN & License Plates (most states)
- Search VIN & License Plates (NY, NJ, PA)
- Find Drivers License Info from name & DOB
- Vehicle History Reports from Car Fax

Miscellaneous People Searches
- A copy of all 3 Credit Bureau Reports
- Web URL Owner Search
- Do-It-Yourself Search Software

children running wild on the internet?

All services provided by:
Intelligent e-Commerce, Inc.
Site protected by copyright © 2003. All rights reserved.

SLIDE 3

Background Checks

For a price list by fax, call (888) 249-5171 or click here.

Most everyone finds the need at one time or another to check someone out. Purposes range from pre-employment checks to pre-marital and pre-litigation inquiries. Background information can be obtained for any legitimate purpose and in most cases does not require the permission of the person being investigated. Many of the following searches require supporting documentation designed to prevent stalking or harassment. In some cases, information will be released only to your attorney.

SERVICES AVAILABLE:

PERSONAL PROFILE REPORT: Compilation of information from numerous databases, returns combination of address history, neighbors, relatives, motor vehicles, real property, judgments, leins, etc.

CRIMINAL RECORDS: Records of criminal convictions are available by county or statewide (19 states) and require the subject's full name, date of birth, and the name of the county or counties to be searched. Some statewide searches require social security number, race and sex.

BOOKING & ARREST RECORDS: Arrest records available in some states. Requires full name, date of birth and social security number.

CIVIL & DIVORCE RECORDS: Records of parties to civil litigation are available by county. These records include civil lawsuits and divorces. Inputs require the subject's full name and the name of the county or counties to be searched. Note that these records may include other persons with the same name, so caution must be exercised when reviewing these records.

FEDERAL RECORDS: Records of parties to federal actions. Must input full name, name of court (i.e. U.S. District Court - Newark N.J,), and choice of felony / misdemeanor and civil / criminal.

ADDRESS HISTORY BY SSN: Provides a list of names and addresses used in connection with a given social security number as reported to credit bureaus during the past seven years.

BANKRUPTCIES, LIENS & JUDGMENTS: Provides records of court-ordered financial obligations by state. Must provide the subject's full name and state to be searched.

DRIVING RECORD: Given a full name, address, date of birth, social security number and drivers license number, will return a driving abstract for that individual (3 years in most states).

CORPORATIONS & LIMITED PARTNERSHIPS: Search by state by 1) individual name, or 2) corporation name for registered affiliations within that state.

CREDIT REPORT: Personal credit reports provide information regarding an individual's credit-worthiness, financial stability, spending habits, prior addresses and more. Obtaining a personal credit report requires a permissible use under the Fair Credit Reporting Act. Inputs require full name, SSN and address.

MILITARY SERVICE: This search determines or verifies the branch and dates of U.S. military service. Input requires full name, address, DOB and SSN.

SLIDE 4

MEDICAL TREATMENT HISTORY: Provides a record of medical visits for up to ten years prior to the date of the search. Identifies name and address of the treating facility and the dates of such treatments. The nature of treatment or exact purpose of the patient's visit is not provided with this search due to privacy regulations. Input requires full name, address, DOB and SSN.

CREDIT CARD ACTIVITY: This search provides a list of purchases made on a given credit card. These purchases will provide information pertaining to the cardholder's spending habits and nature of his/her expenditures. You provide the cardholder's name, all identifiers and the complete card number, we provide the vendor's name with dates and amounts of purchases made in a given period.

TELEPHONE RECORDS: This search provides access to records of calls made from a given number, which provides the researcher with a list of "associates" and "contacts" which often reflect the activities and habits of the person making the calls. Must have legitimate and documented purpose for access to these records.

BANK ACCOUNT HISTORY: This search will provide a history of activity in a given checking or savings account, including dates and amounts of deposits, checks written, wire transfers, significant transactions and monthly account balances. Must have legitimate and documented purpose for access to these records.

EMPLOYMENT HISTORY: Searches are for current employment information and for past employers. FCRA documentation is required. Call for details.

AIRLINE TRAVEL RECORDS: Given someone's name and vitals, this search will identify flights taken by that person. We can search individual airlines, airports, and travel agencies during a specified time frame for recent activity. (Note: Passenger lists by flight are not available)

[Research Services] [Investigative Services in NJ & PA]
[P.I. Training Academy] [Investigative Training Books]

Copyright © 2003 Advanced Research, Inc. - All Rights Reserved.
Hosted and Maintained by PI-WEB-HOST

SLIDE 4

How To Use This Site
- First Time User
- Returning Clients
- Client Agreement

Investigation
- All Searches
- People Searches
- DMV Searches
- Telephone Searches
- Asset Searches
- Criminal Searches
- Civil Searches
- Business Searches
- Dossiers

Client Area
- Check Order Status
- View Search Results
- Client Support

Media Center
- What Clients Are Saying
- What The Media Is Saying

- **Site Map**
- **Free Resources**
- **Privacy Statements**

DOCUSEARCH is the America's premier provider of on-line investigative solutions. Requesting investigative services has never been easier than using our web site. All functions are available with a simple point and click. Our user-friendly interface will prompt you for all the necessary data. Once an assignment is complete, you will be notified by email that the results have been posted in a secure, password protected client area. It doesn't get any easier than that!

In the rather crowded field of search services and information brokers, Docusearch has achieved distinction through profiles in Forbes magazine and widely recognized television media. Most recently, we won further accolades as Forbes Favorite Web Site.

Obtaining the critical information you need has never been easier. Give us a try, you won't be disappointed!

Important: Not all searches are available to the public. Some are reserved for the investigative and legal industry. Docusearch.com reserves the right to refuse conducting any search to anyone at anytime. Prices are subject to change without notice.

Web Site Reviews Forbes Selection

2004 Best Of The Web!

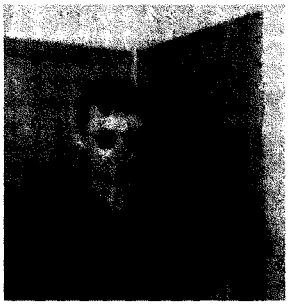
Once again, Docusearch is Forbes Favorite Web Site for 2004. But don't take our word on it...

Read the review

To celebrate, we have reduced the prices of two of our most popular searches. The Cellular Phone Lookup has been cut from $99 to **$45**. Also, the Comprehensive Background Dossier has been expanded to include much more information and the price reduced from $129 to **$59**.

SLIDE 5

Greetings Infidels, I am Liam Youens



Who am I? Well if i had 20 people buried in my backyard my neighbors would have described me as "Quiet, basically kept to himself".

My life from birth to February 1995

What I was thinking during my senior year

What happened after Highschool
first year
second year
third year

I would just like to say that.. people are idiots and the world is full of bullshit. People who commit murder like this are never considered 'justified' nor will I, but who's going to stop me, you might as well murder me yourself. The people on Woodbury Drive are 'Protecting' Amy and say -> 'we make Amy safe from Liam..' ooo you put the cars off the street thats sooo scarey.., The NPD believed it could prevent me from getting guns HA! like that incident would make me change my mind, and they accually believe it. Some people thought that me working at 7-11 was hilarious, Idiots! the only reason I would get that job would be to spend every cent I earned on powerful assualt rifles to execute my vengence. As for Graeme's story I know exactly what he was saying to me, as if I didnt already view all perspectives. What a fool to think that I was That type of person, I have Always lusted for the death of Amy. Guess what Graeme I was depressed not for the love of Amy, but because I was unable to Kill her in school. How Pathetic Graeme and Bethanie are. Amy too, although she eventually realized I would kill her, she did not know that whatever she or anyone else did, it would not change my state of mind. Amy ruined her friendship with Bethanie for no reason.

Too bad for Amy that she now has the mind set of the NPD, Woodbury drive res. and most people in the class of 97. As some of them believe I am no threat to her and that I'm just a fuck-up (or in a more simpathetic way - "I am re-evaluate my my life.." cough.. bullshit). I would Never just stand idle and watch the world go bye. See people are idiots that can not read others effectively.

SLIDE 6

I was made fun of in High School eh.. teen anist? Hardly.. what cowardly primate behavour. What I did to Amy was Nothing compared to the Gang rape of that NHS student a few years ago, somehow I'm to be critized for what I did, when they got a 'well we just have to see if it's true or not'? Ha! Am I supposed to listen when people say 'show some Respect' when I Know that their logic is corrupt, hippocritical, and lie based? Ha! And no one will Ever tell me that I am in the wrong by using a faith based or an artificial societal idea that murder is just wrong under no circumstance? I am Far too superior to consider that.

When Luke Woodham went on his rampage, people called his note 'rambling' and said the shooting was a boyfriend-girlfriend thing. Ha! what an obvious attempt to put him beneth you. You know full well that he would Never have done it if he was not psychologically abused in school reguardless of a passed relationship, but because that is the status-quo of society you play it down! Again and again the same, but you figured out that you were only causing more shootings. Then Columbine.. they got crosses! arent they just murders? they're adults arent they? Now you even said "This is what people do to change society, it has happened before in American history." No one called them Copy-cat shooters, but thats exactly what they are by your logic! Call their journal rambiling, say it was a copy-cat thing! You would try to put Eric and Dylan beneth you, but you know it would just cause more killing.. why more? because your Wrong, your just too stupid to realize it.

**note: 'you' refers to anyone who would Dare attempt to judge me, not including those who know me personally - personally being a relative term of course.

Why am I killing her?
Why am I killing her?
Why am I killing her?

I don't love her anymore, I wish I did but I don't. I wish I could have killed her in Highschool. I need to kill her so I can transport myself back into highschool. I need to stop her from having a life. But why her and not someone else? If I had a life myself, I really wouldn't care even if I was in love with her. Is it the reaction of other people and there attempts to 'punish' me, where I say, "poor baby, I have suffered 10 times as much (at the hands of others too)"? That would be the main reason, but I don't really 'care' per se. Is it the sense of 'beating' the cops (and woodbury dr. res., even her family too) and to know I succeded where they failed? It's amazing that when I wasn't able to kill her I was freaking out, totally obsessed with her death, But when I know I have her I imediately calm down. My emotions then run low and my thoughts change. When I wrote what your reading right now, I knew I had her. If I was still conserned about having access to her I wouldn't have written this part; I would be freaking out and saying, "I Must Kill her.. Fuck!"

I have had idea's about killing Amy. I had been trying to kill Owen this past year, but I didn't have the courage to shoot him. I would have to wait until next semester. At that point Amy may have moved out of her parent's house, giving me the option of killing her at her new home, before proceding to UNH and killing Owen. I went on the 1800ussearch website again (see 'after highschool third year') to do just that. I really had to find out her apt. number on Woodbury Drive this time, because without the apt. number I wouldn't get a 'hit' in the search for her new address, so I buckled down and read the phone book ..again. I needed to find out what the addresses were on the whole street so I could pin-point Amy's. I knew the house was 4th on the left. When I finished finding Woodbury Drive residents in the phone book I thought my best bet was apt. number 7 so I entered the information. It wasn't 7, but who cares I got a HIT! I fell to the floor and let the endorphines fly. Her address was 10 Woodbury Drive she didn't move from home yet, no other information was provided in the background check.

I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment. It's accually obsene what you can find out about a person on the internet. I'm waiting for

SLIDE 6

he results..

My Guns

Youth Group people

Mass Murder

Misc.

SLIDE 6

News From:

U.S. Senator
Russ Feingold

506 Hart Senate Office Building
Washington, D.C. 20510-4904
(202) 224-5323

http://www.senate.gov/~feingold

Contact: **Trevor Miller**
(202) 224-8657

Statement of U.S. Senator Russ Feingold

At the Senate Judiciary Committee Hearing on
"Securing Electronic Personal Data: Striking a Balance
Between Privacy and Commercial and Governmental Use"

April 13, 2005

Mr. Chairman, thank you very much for holding this hearing today. This is an extremely important issue, and one that I am very pleased the Judiciary Committee is taking up.

Recent security breaches at companies like ChoicePoint and Lexis-Nexis, which collect and sell information about individuals, have placed the identities of hundreds of thousands of Americans at risk. Congress needs to understand how and why these security breaches happened, something I hope we can begin to accomplish at today's hearing, and whether a new legal regime is needed. There is no question that data aggregators provide valuable services, allowing consumers to obtain instant credit and police officers to locate suspects. But these companies also gather a great deal of potentially sensitive information about individuals, and in many instances they go largely unregulated.

However, this is about much more than just information security. Until California law required ChoicePoint to notify individuals that their information was compromised and they might be vulnerable to identity theft, many Americans had never heard of this company. As news stories focused on the data broker business, many Americans were surprised to discover that companies are creating digital dossiers about them that contain massive amounts of information, and that these companies sell that information to government and business entities. The revelations about these security breaches highlighted that Americans need a better understanding of what happens to their information in a digital world – and what kind of consequences individuals can face as a result.

1600 Aspen Commons
Middleton, WI 53562
(608) 828-1200

517 E. Wisconsin Ave.
Milwaukee, WI 53202
(414) 276-7282

First Star Plaza
401 5th St., Room 410
Wausau, WI 54403
(715) 848-5660

425 State St., Room 232
La Crosse, WI 54603
(608) 782-5585

1640 Main Street
Green Bay, WI 54302
(920) 465-7508

In particular, I am concerned about an aspect of the data broker business that has not yet gotten much attention in the wake of these security breaches. The information gathered by these companies is not just sold to individuals and businesses; law enforcement agencies like the FBI also buy or subscribe to information from commercial sources.

While I believe the government should be able to access commercial databases in appropriate circumstances, there are no existing rules or guidelines to ensure this information is used responsibly. Nor are there any restrictions on the use of commercial data for powerful, privacy-intrusive data mining programs. The Privacy Act does not apply because the information is held outside the government and is not gathered solely at government direction.

As a result, there is a great deal we do not know about government use of commercial data, even in clearly appropriate circumstances such as when the agency's goal is simply to locate an individual already suspected of a crime.

We don't know under what circumstances government employees can obtain access to these databases or for what purposes. We don't know how government agencies evaluate the accuracy of the databases to which they subscribe, or how the accuracy level affects government use of the data. We don't know how employees are monitored to ensure they do not abuse their access to these databases, or how those who misuse the information are punished. We don't know how government agencies, particularly those engaged in sensitive national security investigations, ensure that the data brokers cannot track the individuals about whom the government is seeking information, an issue that is particularly important in light of the security problems we are talking about today.

The lack of information about government use of commercial data is even more worrisome in the context of data mining programs. A government law enforcement or intelligence agency searching for patterns of criminal or terrorist activity in vast quantities of public and private information raises serious privacy and civil liberties issues – not to mention questions about the effectiveness of these types of searches. More than two years after Congress first learned about Total Information Awareness, there is still much we do not know about the federal government's other work on data mining.

That is why I am planning to reintroduce in the next few days my Data Mining Reporting Act, which would require all federal agencies to report to Congress on data mining programs used to find a pattern indicating terrorist or other criminal activity and how these programs implicate the civil liberties and privacy of all Americans. The bill does not end funding for any program, does not determine the

rules for use of the technology or threaten any ongoing investigation that uses data mining technology. But it would allow Congress to conduct a thorough review of the costs and benefits of the practice of data mining and make considered judgments about which programs should go forward and which should not.

I am glad that this hearing gives us an opportunity to explore both government and commercial reliance on data brokers, and I look forward to working with my colleagues on the Committee to develop legislation to address these issues.

News from . . .

Senator Dianne Feinstein

of California

FOR IMMEDIATE RELEASE:
Wednesday, April 13, 2005

Contact: Howard Gantman
or Scott Gerber 202/224-9629
http://feinstein.senate.gov/

Feinstein Testifies on Recent Data Breaches
ID Theft Notification Bill at Judiciary Committee Hearing

***Washington, DC** – At a Senate Judiciary Committee today, U.S. Senator Dianne Feinstein (D-Calif.) called on the Senate to approve legislation that she has sponsored to ensure that consumers are notified when their personal information is compromised in such a breach.*

Senator Feinstein's legislation requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver's license or state identification number, or credit card or bank account information – has been compromised. Only two exceptions to notification exist. First, upon the written request of law enforcement for purposes of a criminal investigation; and second, for national security purposes.

The following is the prepared text of her statement:

"Thank you Chairman Specter and Senator Leahy for giving me the opportunity today to testify on behalf of the 'Notification of Risk to Personal Data Act of 2005'.

I strongly believe that the notification bill that I re-introduced Monday afternoon (S. 751) – and which is a strengthened version of S. 115 that I introduced in January – is necessary to help protect Americans from the vast and growing crime of identity theft. This bill will ensure that Americans are notified when their most sensitive personal information – their Social Security Number, their driver's license or state identification number, their bank account and credit card information – is part of a data breach putting them at risk of identity theft.

Just yesterday, we learned that LexisNexis underreported the number of individuals whose personal information may have been stolen in March of this year. Instead of 32,000 individuals being potentially affected by the breach at its newly acquired Seisint unit, 310,000 people nationwide may have been affected and their personal data stolen.

But since February 2004 alone, there have been at least 12 major breaches of databases which has placed 10.7 million people in jeopardy of identity theft. These are just the cases that we know about. Who knows the impact of the cases that we don't. And there were 9.3 million reported cases of identity theft last year alone, including 1 million in California.

So what can we do? We urgently need a strong national standard that says whenever a data system is breached, everyone who is at risk of identity theft must be notified.

Here's what the bill does: It requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver's license, or credit card number – has been compromised.

Only two exceptions to notification exist. First, upon the written request of law enforcement for purposes of a criminal investigation; and second, for national security purposes.

This bill is based on the ground-breaking California law which is the first and only State law requiring notification of individuals. The California law really opened our eyes to the problem. Without it, we probably wouldn't have heard about half of the cases I mentioned before.

But in fact, the legislation I'm introducing today is much stronger than the California law. **Here's how:**

- It covers both electronic and non-electronic data – as well as encrypted and non-encrypted data. The California law only includes unencrypted, electronic data.

- It allows individuals to put a 7-year fraud alert on their credit report. The California law doesn't address fraud alerts.

- It doesn't include a major loophole allowing companies to follow weaker notification requirements – as the California law does.

- It lays out specific requirements for what must be included in notices, including:

    - a description of the data that may have been compromised;
    - a toll-free free number to learn what information and which individuals have been put at risk;
    - and the numbers and addresses for the three major credit reporting agencies.

- By contrast, California law is silent on what should be in notices.

- It has tougher civil penalties -- $1,000 per individual they failed to notify or not more than $50,000 per day while the failure to notify continues or existed. In California, a victim may bring a civil action to recover damages or the company may be enjoined from further violations.

- And most importantly, it sets a national standard – so that individuals in Iowa, Oklahoma, and Maine have the same protections as consumers in California.

- The law would be enforced by the Federal Trade Commission or other relevant regulator, or by a State attorney general who could file a civil suit.

And because the bill is stronger than California law, leading privacy groups – including Consumers Union and the Privacy Right's Clearinghouse – have endorsed this legislation.

You can't tell the true impact of identity theft by looking at the numbers. You see it in the stories of the victims. Let me tell you how identity theft works.

While Rebecca Williams was living in San Diego in April 2000, a thief was using her Social Security number, her birthdate, and her name to establish a parallel identity thousands of miles away in the Chicago area.

The thief opened a household, obtained a driver's license, and signed up for credit cards in her name. The thief even tried to use her identity to purchase a car. In all, the thief used Ms. William's identity to open more than 30 accounts, accruing tens of thousands of dollars worth of goods and services. Sometimes accounts were opened despite the fact that fraud alerts had been issued.

Ms. Williams says that restoring her identity is "like a full-time job" and estimates that she has spent the equivalent of 8-hours a day for three full months working with credit bureaus, credit card companies, and various government agencies trying to put her life back together.

But five years later, Ms. Williams still has not fully restored her identity – she faces two civil judgments for unpaid rent for apartments she never lived in, she faces higher interest rates for loans and credit cards, and she lives in fear that the thief, who has never been caught, will once again use her identity as a source of income.

This is not an isolated incident. This is happening in every community across the country. Sometimes it is an individual acting alone. Other times it is part of an identity theft ring. But in every case, there is a victim who has been violated in an extremely personal way.

I strongly believe individuals have a right to be notified when their most sensitive information is compromised – because it is truly their information. This bill will give all Americans more control and confidence about the safety of their sensitive personal information.

It will help combat the growing scourge of identity theft. And if an identity theft does occur, it will give individuals the ability to protect themselves from further fraud. I look forward to working with my colleagues to pass this critically important legislation.

Thank you, Mr. Chairman and Senator Leahy."

###

Statement of Mr. Larry Johnson

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Presentation to the Senate Committee on the Judiciary

United States Senate

April 13, 2005

Good afternoon, Chairman Specter. I would like to thank you, as well as the distinguished Ranking Member, Senator Leahy, and the other members of the Committee for providing an opportunity to discuss the subject of information security, and the role of the Secret Service in safeguarding our financial and critical infrastructures.

Background

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. With the passage of new federal laws in 1982 and 1984, the Secret Service was provided primary authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

After 138 years in the Department of the Treasury, the Secret Service transferred to the Department of Homeland Security (DHS) in 2003 with all of our personnel, resources and investigative jurisdictions and responsibilities. Today, those jurisdictions and responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

The expanding use of the Internet and the advancements in technology, coupled with increased investment and expansion, has intensified competition within the financial sector. With lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokerage. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information. In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize is a valuable commodity in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects and such efforts can significantly limit the opportunities for identity crime.

The methods of identity theft utilized by criminals vary. "Low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving." The theft of wallets, purses and mail is also a widespread practice employed by both individuals and organized groups.

With the proliferation of computers and increased use of the Internet, "high tech" identity criminals began to obtain information from company databases and web sites. In some cases, the information obtained is in the public domain, while in others it is proprietary and is obtained by means of a computer intrusion or by means of deception such as "web-spoofing" or "phishing".

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a utility billing center, financial institution, medical office, or government agency. The collusive employee will access the proprietary data base, copy or download the information, and remove it from the workplace either electronically or simply by walking it out.

Once the criminal has obtained the proprietary information, it can be exploited by creating false "breeder documents" such as a birth certificate or social security card. These documents are then used to obtain genuine, albeit false, identification such as a driver's license and passport. Now the criminal is ready to use the illegally obtained personal identification to apply for credit cards or consumer loans or to establish bank accounts, leading to the laundering of stolen or counterfeit checks or to a check-kiting

scheme. Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

Agency Coordination

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Members of these task forces, including representatives from local and state law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which authorized the Secret Service (pursuant to the USA PATRIOT Act of 2001) to expand our Electronic Crime Task Forces (ECTF) initiative to cities and regions across the country. Additional ECTFs have been added in the last two years in Dallas, Houston, Columbia (SC), Cleveland, Atlanta and Philadelphia, bringing the total number of such task forces to 15.

The Secret Service ECTF program bridges the gap between conventional cyber-crimes investigations and the larger picture of critical infrastructure protection. Secret Service efforts to combat cyber-based assaults that target information and communications systems supporting the financial sector are part of the larger and more comprehensive critical infrastructure protection and counterterrorism strategy.

As part of DHS, the Secret Service continues to be involved in a collaborative effort targeted at analyzing the potential for financial, identity and electronic crimes to be used in conjunction with terrorist activities. The Secret Service takes great pride in its investigative and preventive philosophy, which fully involves our partners in the private sector and academia and our colleagues at all levels of law enforcement, in combating the myriad types of financial and electronic crimes. Central to our efforts in this arena are our liaison and information exchange relationships with the U.S. Immigration and Customs Enforcement (ICE), the Department of the Treasury, the Department of State, the Federal Bureau of Investigation and our Joint Terrorist Task Force participation.

The Secret Service is actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice (DOJ). This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional organizations, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

In a joint effort with DOJ, the U.S. Postal Inspection Service, the Federal Trade Commission, the International Association of Chiefs of Police and the American Association of Motor Vehicle Administrators, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last two years we have held seminars in eighteen cities nationwide including Denver, Colorado; Raleigh, North Carolina; Orlando, Florida; Rochester, New York; and Santa Fe, New Mexico. Identity Crime seminars scheduled for the upcoming months include Boise, Idaho; Providence, Rhode Island; and Baltimore, Maryland. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

It is through our work in the areas of financial and electronic crime that we have developed particular expertise in the investigation of credit card fraud, identity theft, check fraud, cyber crime, false identification fraud, computer intrusions, bank fraud, and telecommunications fraud. Secret Service investigations typically focus on organized criminal groups, both domestic and transnational. As Secret Service investigations uncover activities of individuals or groups focusing on doing harm to the United States, appropriate contact is immediately made and information is passed to those agencies whose primary mission is counterterrorism.

Finally, the best example of interagency and multi-jurisdictional cooperation came on October 24, 2004, when the Secret Service arrested 30 individuals across the United States and abroad for credit card fraud, identity theft, computer fraud and conspiracy. These suspects were part of a multi-count indictment out of the District of New Jersey and were involved in a transnational cyber "organized crime" underground network that spanned around the world. In addition to the 30 arrests, 28 search warrants were served simultaneously across the United States. Internationally, 13 search warrants were served in 11 different countries in conjunction with this Secret Service-led investigation. Central to the success of this operation was the cooperation and assistance the Secret Service received from local, State and other federal law enforcement agencies as well as our foreign law enforcement partners and Europol.

This case began in July of 2003, when the Secret Service initiated an investigation involving global credit card fraud and identity fraud. Although the catalyst for the case came from a more "traditional" crime of access device fraud, the case evolved into a very technical, transnational investigation. The aforementioned criminal activity primarily

occurred over the Internet. After the initial act(s) of fraud, suspects would exchange contraband (such as counterfeit credit cards and counterfeit driver's licenses). This case, entitled Operation Firewall, developed into a multilateral effort involving 18 Secret Service domestic offices and 11 foreign countries. As the lead investigative office, the Secret Service Newark Field Office conducted a complex undercover operation involving the first ever wiretap on a computer network.

Chairman Specter and Senator Leahy, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Statement of
Arkadi Kuhlmann
CEO, ING DIRECT

Submitted for the Record
April 13, 2005
To the United States Senate, Judiciary Committee
Hearing Concerning the Securing of Electronic Personal Data

Mr. Chairman, I am Arkadi Kuhlmann, CEO of ING DIRECT, a federally chartered thrift headquartered in Wilmington, Delaware. ING DIRECT launched in the U.S. in September 2000 to challenge traditional banking by touting the high interest, no fee and no minimum Orange Savings Account as its signature product, with a brand vision to lead Americans back to saving.

ING DIRECT has since expanded its product line to include the Orange Mortgage, the Orange Home Equity Line of Credit, Orange CDs and the Orange Investment Account. With over 2.5 million customers and more than $43 billion in assets, ING DIRECT is the fourth largest thrift in the U.S.

Identity theft is the most common and fastest-growing crime in the U.S. today. The ability to protect one's personal data is rapidly becoming a top concern for almost every American. The problem of identity theft threatens the economic viability of the financial services sector, as well as many other business sectors.

At ING DIRECT, we know that identity theft and concern over security surrounding private information are top of mind for our customers due to the hundreds of emails and phone calls we receive each year. In 2004, ING DIRECT took the step of establishing its own identity theft assistance program. This program is free of charge and is offered to our customers as well as anyone else we may discover who has been victimized. When contacted, we will stay with the person through every step necessary to restore their identity. To further educate our customers, we have made identity theft and security a core topic addressed in the last seven of eight issues of our Customer newsletter, BrightSpots (published quarterly).

We believe that it is time for the enactment of a federal law that would give us all the ability to control the use of our personal information by third parties. Such a law would help prevent identity thieves from using established means and methods to impersonate others for the purposes of establishing credit or defrauding the victims.

Such a law would give every American the right to block access to her/his credit report for the purpose of extending new credit. Commonly called a security freeze, this approach would prevent an identity thief from establishing a credit card or other loan account in the name of someone else.

The security freeze, as adopted by a small number of states, does not apply to existing accounts or credit relationships, thus allowing current creditors to monitor their customers' credit status. It also does not prevent pre-screening for purposes of making new offers of credit or credit-monitoring requested by the person himself.

We also believe the security freeze should apply to sensitive personal information bought and sold by information brokers. Americans have the right to know who is accessing their information and should have the ability to control that access.

ING DIRECT also supports proposed laws that would require businesses to notify their customers in the case of a breach of data security that has compromised the customers' sensitive personal information. When it comes to the "need to know," institutions should not be allowed to substitute their judgment for that of the individual whose information has been compromised.

In short, until we all take seriously the threat to electronic commerce posed by identity theft and return the control of their private information back to consumers, we will only suffer more and more devastating consequences.

Thank you for the opportunity to present our views.

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, COMMITTEE ON THE JUDICIARY
HEARING ON "SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE"
APRIL 13, 2005

Mr. Chairman, I applaud your decision to hold today's hearing on the challenges we face in securing electronic personal data in a digital era. Earlier this year I wrote to you and requested this hearing, and I appreciate your receptiveness, interest and prompt agreement.

I welcome the witnesses here today and look forward to their testimony. Our colleague, Senator Feinstein, has been a leader on these important issues and I look forward to hearing of her efforts to date, and Senator Schumer and other members of our Committee, as well as Senator Nelson on Commerce, have also followed these issues closely and have insights to offer. I am also pleased to see here today my old friend and fellow Vermonter, Bill Sorrell, who is the Attorney General of Vermont and now is president of the National Association of Attorneys General.

Personal Information, A Hot New Commodity

In the past few months, we have become aware of a string of major security breaches involving large firms such as ChoicePoint, Bank of America and Seisint, a LexisNexis subsidiary. These incidents demonstrate the susceptibility of our most personal data to relatively unsophisticated scams and logistical mishaps, and they raise broader concerns about the misappropriation of personal information and identity theft. The ChoicePoint breach was especially troubling for its highlight of a dangerous vulnerability in the information economy – the inadequate screening of the customers who are buying this personal information. ChoicePoint's bread-and-butter business includes identity verification and screening to help corporate America "know its customers." Yet the company failed to know its own customers and sold personal information on at least 145,000 Americans to criminals posing as legitimate companies.

Advanced technologies, combined with the realties of the post-9/11 digital era, have created strong incentives, opportunities and a robust market for collecting and selling personal information about each and every American. Today, all types of corporate and governmental entities routinely traffic in billions of digitized personal records about Americans. The sudden rise of giant data brokers has brought much of this information together for centralized access. We rely on this data to facilitate financial transactions, provide services, prevent fraud, screen employees, investigate crimes, and find loved ones. In today's security-saturated environment, our own government is using it to "know its residents."

These advances have improved our lives and made us safer. But in this era where personal information has become a key commodity, the personal information of

Americans has become a treasure trove, valuable and vulnerable, and our privacy and security laws have not kept pace.

Increasingly, those who trade in digital dossiers have no direct relationship with the individuals and faces behind the numbers or letters that identify them, so the normal market discipline of disgruntled consumers does not necessarily save the companies from themselves. Even where there is a direct relationship, individuals often have no idea what companies are doing with their personal data or even what kinds of information is being collected about them. What are these companies doing with this information, who do they sell it to, and why? How is it protected? What are the benefits for Americans whose information has become a new commodity? These are all questions that too often go unanswered, with unfortunate, and sometimes tragic, results.

An example of tragic consequences from the misuse of personal data is the case of Amy Boyer. In 1999, a man who had been obsessed with her since high school bought Amy's Social Security number, work address and other information from data broker Docusearch for $154. He came up to her as she was leaving work and fatally shot her, just before killing himself.

In this information-driven age, the use of personal data has significant consequences for every American. People have been refused jobs because a database search has wrongly reported that they have a criminal history. For others caught up in the endless cycle of watching their credit unravel, undoing the damage caused by security breaches and identity theft becomes life-consuming. Last year, 9.3 million Americans fell victim to identity theft, resulting in losses of more than $52 billion to individuals and corporations. And on average, it took 28 hours to sort out the subsequent problems, and much, much longer for many victims.

Sophisticated Scams In The Digital Age

While dumpster-diving is still a popular method of data theft, increasingly the focus is on a new low-hanging fruit: insecure, where one good "hit" nets troves of information. Insecure databases are now low-hanging fruit for hackers looking to steal identities or otherwise misuse data for financial gain. This is especially true as more and more of Americans' personal information is being processed abroad. Just this past weekend, it was reported that individuals working for an Indian data processor stole personal information of Citibank customers and transferred $350,000 to fake accounts. Last year was the report that a Pakistani transcriber of medical files from a San Francisco hospital threatened to post that information on the Internet unless she received back pay.

In yet another strain of cyber crime and high-tech law-breaking, we are seeing a rise in organized rings that target personal data to sell in online, virtual bazaars. These are not your run-of-the-mill criminals. They increasingly have sophisticated computing skills and steal data using a full suite of malicious software, or "malware," such as Trojan horses, keystroke logging, spyware, and phishing, which I recently introduced a bill (S.472) to combat.

A recent investigation by the U.S. Secret Service revealed that one criminal group with some 4,000 members – Shadowcrew -- traded more than one million stolen credit-card numbers, resulting in financial losses of more than $4 million. These are challenging scams to penetrate, and I appreciate and applaud all the work that the Secret Service and other federal agencies have been doing to crack these cases. Just recently, the Senate Sergeant of Arms posted guidance on identity theft on the Senate website.

State and local law enforcement have also worked tirelessly to combat cyber challenges. I know in Vermont, the U.S. Small Business Administration will be hosting a forum to protect small businesses from the impact of scams and identity theft.

Identity theft is a major problem, but when the government is the purchaser of personal data, citizen inconveniences have also arisen, and the stakes can be far higher. We have all heard stories from everyday individuals, as well as colleagues like Senator Kennedy, about the airline passenger screening programs that use incomplete or bad data to peg innocent individuals for delay or denied boarding.

Protecting National Security As Well As Financial Security

Weaknesses in the data industry can also jeopardize our law enforcement and homeland security efforts. Government contractors providing critical data and processing tools must get it right. Protecting our borders requires that we prevent security breaches, especially as we outsource data abroad, that would allow a potential terrorist to steal Social Security and account numbers and masquerade as law-abiding residents, or simply fund their criminal enterprises. We also need to know that data brokers are safeguarding the secrecy of law enforcement investigations and operations where necessary. For example, we need to ensure that there are no technological weaknesses in the data brokers' systems that are supposed to prevent their employees from viewing FBI data searches and suspects the Bureau is investigating.

Our hearing today is not about shutting down these data brokers or abandoning their services. It is about shedding a little sunshine on current practices and weaknesses, and establishing a sound legal framework to ensure that privacy, security and civil liberties will not be pushed aside in this new and evolving age.

Today will be an opportunity to address these concerns as we hear from some of the industry's leaders, ChoicePoint, Acxiom and LexisNexis. These companies play a legitimate and valuable role in the information economy. Their data services facilitate important commercial transactions, improve hiring decisions, deter fraud, assist law enforcement and enhance homeland security. But as with any other significant beneficial industry, the information industry is subject to mistakes, abuse, and unintended consequences that can flourish absent transparency, oversight and proper boundaries.

Although we are focusing today on several leading data brokers, many other companies that traffic in personal data use much lower standards than the companies that have

agreed to come under the spotlight today. For example, Docusearch, the company that sold Amy Boyer's personal information to her killer, has said it has no duty to check its customers' backgrounds. This past December, CNN interviewed the founder of Abika, an Internet-based company that performs some three million background searches annually and creates psychological profiles. He said, "I don't even believe in privacy too much . . . why do we need privacy? That's the question . . . why do people need privacy?"

That kind of sentiment is outrageous and is not one that should be tolerated in the data industry. But I will answer the question. One of the most fundamental liberties of being an American is the right to be let alone, and when you invade someone's privacy or treat it glibly, you trample on that liberty. That's why we need privacy, and that's why we should vigilantly protect it.

A Role For Congress

Congress has a role in protecting Americans' privacy, but we need to do it right. Senator Specter and I, as well as many others on the Committee, have been examining these issues closely to ensure a carefully balanced environment that can evaluate the adequacy of current boundaries and behaviors in the realm of data brokering.

We need to consider rules that will guarantee Americans the right to see what information has been collected about them and to make corrections where necessary. We need to consider rules that will ensure Americans are notified when there has been a security breach involving their digitized personal information. We also need to create baseline expectations for data security programs and practices, and penalize government contractors that don't comply. We also need to look at how to protect increasingly public, yet vulnerable, sensitive data such as Social Security numbers, which are the keys to unlocking so much of our financial and personal lives. A computer glitch at another payroll company, PayMaxx, allowed any of its customers to see thousands of W-2s of other company clients, including social security numbers and salaries. Just this past week, it was reported that "Automatic Data Processing," a company that provides payroll and benefits to corporations, mailed out postcards to 1000 workers with their Social Security numbers brazenly visible for anyone to see. Worse still, they described in detail how those Social Security numbers could be used to access employee benefits online. This should not happen. We must have a national dialogue on when and how Social Security numbers can be properly used.

Finally, we need to take a closer look at how the government is using commercial data, and whether those uses properly balance privacy and civil liberty concerns. Recently a ChoicePoint executive was quoted as saying, "We do act as an intelligence agency, gathering data, applying analytics." These partnerships between governments and private data brokers create new challenges for maintaining privacy standards over sensitive information involving each and every American.

With such powerful information-age tools comes heightened responsibility. As the 9/11 Commission noted, "...we must find ways of reconciling security and liberty, since the success of one helps protect the other." No doubt, the information industry can enhance law enforcement and homeland security efforts. But as the Commission also recognized, "while protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing act is no easy task, but we must constantly strive to keep it right." We can "keep it right" by putting mechanisms in place to ensure appropriate checks and balances and congressional oversight.

We have many issues to consider on this front. Today's hearing will begin that process by shedding much-needed light on a rapidly growing industry and its practices of handling the most personal information of each and every American.

#####

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON THE JUDICIARY

U.S. SENATE

on

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

April 13, 2005

I. INTRODUCTION

Mr. Chairman, 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

---

[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).

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.

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

---

[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.

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.

---

[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.

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
- 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

---

[5] 15 U.S.C. §§ 1681-1681u, as amended.

[6] 15 U.S.C. §§ 6801-09.

[7] 15 U.S.C. § 45(a).

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 requires 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

---

[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).

"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

---

[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).

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

---

[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.

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]

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

---

[18] 15 U.S.C. § 1681f. The information a government agency may obtain under this provision does not include Social Security numbers.

[19] 15 U.S.C. §§ 1681u, 1681v.

[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).

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

---

[23] *Id.*

[24] A press release describing the consent agreement is available at: http://www.ftc.gov/opa/predawn/F93/irsc-cdb-3.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).

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 prevention, 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

---

[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).

[31] 15 U.S.C. § 6802(e).

[32] 16 C.F.R. § 313.11(a).

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

---

[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,

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.

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).

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 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

---

[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).

[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).

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

---

[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").

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 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

---

[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).

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 1.8 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

---

[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).

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 809,000 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 over 815,000 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

---

[51] Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Feb. 2005) (available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf).

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 17 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 Financial 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.

---

[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.

New York's Senator

CHARLES E. SCHUMER

313 Hart Senate Office Building • Washington, DC 20510
Phone: (202) 224-7433 • Fax: (202) 228-1218 • Web: *schumer.senate.gov*

FOR IMMEDIATE RELEASE
April 13, 2005

CONTACT: Israel Klein
(202) 224-7433

SCHUMER INTRODUCES COMPREHENSIVE ID THEFT BILL; IDENTITY THEFT AT LEXIS NEXIS 10X'S LARGER THAN EXPECTED

Recent Examples of Egregious Loopholes That Are Compromising Personal Information Need Immediate and Thorough Action by Congress

Schumer-Nelson Bill Would Empower FTC, Inform Consumer to Prevent ID Theft in Future, Not Just Punish Wrongdoers after the Fact

On the heels of numerous and significant identity theft breaches, U.S. Senators Charles E. Schumer (D-NY) and Bill Nelson (D-FL) introduced major and comprehensive legislation last night to prevent ID theft, to give broader authority to the Federal Trade Commission, and require more disclosure. The Schumer-Nelson ID Theft Prevention bill is the first and most comprehensive effort to really prevent ID theft, not just punish those who commit ID theft. Sen. Schumer is a member of almost all the committees that would have jurisdiction over this bill including the Finance, Judiciary, and Banking Committees, and Sen. Nelson is a member of the Commerce Committee, which also has jurisdiction.

Schumer said, "What bank robbery was to the Depression Age, identity theft is to the Information Age. Identity theft has become so pervasive and so out-of-hand, that we must make a real effort to prevent it before it happens. When a company like Lexis-Nexis so badly underestimates its own ID theft breaches, it is clear that things are totally out of hand."

According to Lexis-Nexis yesterday, they found a 300,000 person sensitive personal information breach, not a 30,000 person breach, which was originally reported last month.

"This bill not only will help stop the erosion of privacy," said **Nelson**, a longtime champion of consumer privacy. "But it also will cut through the red tape identity theft victims now face when they try to restore their credit."

Schumer continued, "Everyone knows that once your identity has been stolen, you can't get it back. That is why our comprehensive measure focuses on making sure that your personal information isn't surfing the Internet without your permission and that companies handling your Social Security number and other sensitive information should come under the watchful eye of the Federal Trade Commission immediately."

Schumer Nelson ID Theft Prevention Bill will:

Create FTC Office of Identity Theft to help the millions of victims of ID theft each year to get their identity back through an easily accessible website, toll free phone number and consumer-service teams, and authorizes $60 million a year, for five years for this office.

Regulate data merchants (akin to regulation of credit bureaus) by:

- Make them register with the FTC;
- Institute safeguards to prevent fraudulent access by unauthorized parties;
- Develop authentication process for their customers with individualized passwords;
- Users allowed these passwords are people who have passed a reasonably effective background check;
- Data Merchant should track who accessed what records and for what lawful purpose they were accessed;
- Allow consumers, like with their credit reports, to obtain reports showing which data-merchants have their information and mandates a correction process to fix errors;
- Demands accuracy standards for their information;
- Regulates Credit Bureaus only if, and as far as, they sell credit header information currently unregulated by the Fair Credit Reporting Act and its amendments.

Disclosure Box:

Any company that is collecting your sensitive personal information and plans to sell or transfer your information to an unaffiliated third party, must put a "Disclosure Box" on it, which lets the consumer know in PLAIN ENGLISH that "this information may be sold or given to an unaffiliated third party without your additional consent."

Notification provisions in the case of an information breach are very similar to current California law (the law that forced ChoicePoint to notify consumers). But there is a new provision, allowing any consumer who is notified of a breach of their information to request, in writing, that their information be completely expunged from the company's database.

Every company required to take "Reasonable Steps" to protect sensitive personal information they are storing.

Social Security Number Specific Provisions:

- Prohibits any company from asking for a Social Security number unless they actually need it in the normal course of business;
- Prohibits SSN's displayed on employee IDs and prohibits inmates in prison from having any access to them as part of their prison jobs;
- Bans SSN purchase and sale, except for law enforcement, national security and fraud purposes;
- Grants U.S. Attorney General the ability to further define the exemptions as situations arise and exempt more if needed.

Would also require the FTC to:

- Study national, state and local governments' public postings of Social Security numbers, come up with recommendations and forward them on to the relevant national, state and local governments;
- Require a thorough annual report each year on ID theft;

- For each section there's a maximum penalty, usually $1,000 per individual record per violation, which can be administered by the FTC or Attorneys General.
- Study international identity theft and determine ways to combat it;
- Create a blue-ribbon working group representing both industry and consumer groups to find the best ways for private entities to protect consumer data;

Stop public postings of private financial account numbers (i.e. mutual fund companies posting shareholder information on Internet).

Preempts state law to the extent that it is inconsistent with the provisions of this bill and then only to the extent of the inconsistency. If the statute offers greater consumer protections than this bill, it shall not be preempted by this bill.

Create an Assistant Secretary for Cyber Security in the Department of Homeland Security, which is what an earlier Schumer amendment to the 9-11 bill and a bi-partisan house bill in the 108th would have done.

# # #

Before the
United States Senate
Committee on the Judiciary

Hearing on
Securing Electronic Personal Data:
Striking a Balance Between Privacy and Commercial and Governmental Use
April 13, 2005

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. I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the use of commercial data.

LexisNexis is a leading provider of authoritative legal, public records, and business information. Today, over three million professionals—lawyers, law enforcement officials, government agencies employees, financial institution representatives, and others—use the LexisNexis services. Government agencies, businesses, researchers, and others rely on information provided by LexisNexis 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:

Preventing identity theft and fraud – Although the insidious effects of identity theft are fairly well known, until recently we did not fully appreciate that identity theft is part of the larger problem of identity fraud. Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It is a component of most major crimes and is felt around the world today. As a result, both industry and government have asked LexisNexis to develop solutions to help address this evolving problem.

LexisNexis remains committed to providing leadership in this area. We recognize the enormity of the problem. In 2004, 9.3 million consumers were victimized by identity fraud.

Credit card companies report $1 billion in losses each year from credit card fraud. With the use of a LexisNexis solution called Fraud Defender, a major bank card issuer experienced a 77 percent reduction in the dollar losses due to fraud associated with identity theft and credit card origination.

LexisNexis products are becoming increasingly necessary to combat identity fraud associated with internet transactions where high dollar merchandise such as computers and other electronic equipment are sold via credit card. Lower fraud costs ultimately mean lower costs and greater efficiencies for consumers.

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. LexisNexis works closely with federal, state and local law enforcement agencies on a variety of criminal investigations. For example, the Beltway Sniper Task Force in Washington, D.C., used information provided by LexisNexis to help locate one of the suspects wanted in connection with that case. In another case, information provided by LexisNexis was recently used to locate and apprehend an individual who threatened a District Court Judge and his family in Louisiana.

Supporting homeland security efforts - LexisNexis worked with the Department of Homeland Security Transportation Safety Administration (TSA) in developing the Hazardous Materials Endorsement Screening Gateway System. This system allows TSA to perform background checks on commercial truck drivers who wish to obtain an endorsement to transport hazardous materials.

Preventing money laundering – LexisNexis has partnered with the American Bankers Association to develop a tool used by banks and other financial institutions to verify the identity of new customers to prevent money laundering and other illegal transactions used to fund criminal and terrorist activities. This tool allows banks to meet Patriot Act and safety and soundness regulatory requirements.

Locating and recovering missing children – Customers like the National Center for Missing and Exploited Children rely on LexisNexis to help them locate missing and abducted children. Since 1984, the Center has assisted law enforcement in recovering more than 85,000 children. Over the past 4 years, information provided by LexisNexis has been instrumental in a number of the Center's successful recovery efforts.

Locating parents delinquent in child support payments – Both public and private agencies rely on 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 the Enforcement of Support (ACES), a private child support recovery organization, has had tremendous success in locating nonpaying parents using LexisNexis.

These are just a few examples of how our information products are used to help consumers by detecting and preventing fraud, strengthening law enforcement's ability to apprehend criminals, protecting homeland security and assisting in locating missing and abducted children.

Types of Information Maintained by LexisNexis Risk Solutions

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 that is available to the general public from non-governmental sources. Telephone directories are an example of publicly available information.

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 credit header data. Credit header data is the non-financial 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.

Privacy

LexisNexis is committed to the responsible use of personal identifying information. We have privacy policies in place to protect the consumer information in our databases. 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 information contained in our databases. We also undertake regular third-party privacy audits to ensure adherence to our privacy policies.

LexisNexis has an established Consumer Access Program that allows consumers to review information on them contained in the LexisNexis system. While the information provided to consumers under this program is comprehensive, it does not include publicly available information such as newspaper and magazine articles and telephone directories contained in the LexisNexis system.

LexisNexis also has a consumer opt-out program that allows individuals to request that information about themselves be suppressed from selected databases under certain circumstances. To opt-out of LexisNexis databases, an individual must provide an explanation of the reason or reasons for the request. Examples of reasons include:

- You are a state, local or federal law enforcement office or public official and your position exposes you to a threat of death or serious bodily harm;
- You are a victim of identity theft; or
- Your are at risk of physical harm.

Supporting documentation is required to process the opt-out request. While this opt-out policy applies to all databases maintained by our recently acquired Seisint business, it is limited

to the non-public information databases in the LexisNexis service. The policy does not currently apply to public records information databases maintained by LexisNexis. We are currently evaluating what steps we can take to better publicize our opt-out program and extend the program to all public records databases in the LexisNexis service.

Security

LexisNexis has long recognized the importance of protecting the information in our databases and has multiple programs in place for verification, authorization and IT security. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities. LexisNexis also 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.

Only those customers with a permissible purpose under applicable laws 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 and we limit a customer's access to information in LexisNexis products according to the purposes for which they seek to use the information.

Maintaining security is not a static process -- it requires continuously evaluating and adjusting our security processes, procedures and policies. High-tech fraudsters are getting

more sophisticated in the methods they use to access sensitive information in databases. We continuously adapt our security procedures to address the new threats we face every day from those who seek to unlawfully access our databases. We undertake regular third-party security audits to test the security of systems and identify any potential weaknesses.

Even with the multi-layer safeguards in place at LexisNexis, we recently discovered that unauthorized persons primarily using IDs and passwords of legitimate customers may have accessed personal identifying information at our recently acquired Seisint business. In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. At that point we contacted the U.S. Secret Service. The Secret Service initially asked us to delay notification so they could conduct their investigation. About a week later we publicly announced these incidents and within a week sent out notices to approximately 30,000 individuals.

The investigation revealed that unauthorized persons, primarily using IDs and passwords of legitimate customers, may have accessed personal-identifying information, such as social security numbers (SSNs) and driver's license numbers (DLNs). In the majority of instances, IDs and passwords were stolen from Seisint customers that had legally permissible access to SSNs and DLNs for legitimate purposes, such as verifying identities and preventing and detecting fraud. No personal financial, credit, or medical information was involved since LexisNexis and Seisint do not collect such information. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated nor was any customer data residing within that infrastructure accessed or compromised.

Based on the incidents at Seisint, I directed our teams to conduct an extensive review of data search activity at our Seisint unit and across all LexisNexis databases that contain personal identifying information. In this review, we analyzed search activity for the past twenty-seven months to determine if there were any other incidents that potentially could have adversely impacted consumers. We have just completed that review. As a result of this in-depth review, we discovered additional incidents where there was some possibility that unauthorized persons may have accessed personal identifying information of approximately 280,000 additional individuals.

We deeply regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify the initial group of individuals and will begin notifying the recently-identified individuals within a few days. We are providing all identified individuals with a consolidated credit report and credit monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity. We will also provide them with identity theft expense insurance coverage up to $20,000 to cover expenses associated with restoring their identity and repairing their credit reports.

We have learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. These include:

- Changing customer password security processes to require that passwords for both system administrators and users be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;

- Suspending customer passwords after five unsuccessful login attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation;
- Further limiting access to the most sensitive data in our databases by truncating SSNs displayed in non-public documents and narrowing access to full SSNs and DLNs to law enforcement clients and a restricted group of legally authorized organizations, such as banks and insurance companies; and
- Educating our customers on ways they can increase their security.

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 personal identifying 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 headers contain the non-financial 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. Credit header data is obtained from consumer reporting agencies.[1] Since July 2001, the compilation of credit header data has been 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

[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.

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 further enhance data security and address the growing problem of identity theft and fraud. LexisNexis supports the following legislative approaches:

Data Security Breach Notification. Consistent with the proposals outlined by FTC Chairman Majoras, 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 has raised about ensuring that there is an appropriate threshold for when individuals 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 legislation

contain federal preemption to insure that companies can quickly and effectively notify individuals 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 supports 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 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.

Information services companies like LexisNexis provide government agencies with critical information that they depend on to do their jobs. It is important that no legislation be enacted that would prohibit or limit government access and use of commercial data. Moreover,

any legislation considered must strike the right balance between protecting privacy and ensuring continued access to critically important information that is provided through information service providers.

I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the use of commercial data. I look forward to working with the members of this committee as you debate these important public policy issues.

PREPARED STATEMENT OF WILLIAM H. SORRELL
VERMONT ATTORNEY GENERAL AND
PRESIDENT OF THE NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

Before the

COMMITTEE ON THE JUDICIARY

U.S. SENATE

on

SECURING ELECTRONIC PERSONAL DATA:
STRIKING A BALANCE BETWEEN PRIVACY AND
COMMERCIAL AND GOVERNMENTAL USE

April 13, 2005

I. INTRODUCTION

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

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

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

II. THE GROWTH OF SECURITY BREACHES

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

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

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

- Ford Motor Credit: In 2002, three individuals were arrested for downloading credit reports on more than 30,000 consumers, and then selling the credit reports to street criminals who emptied the victims' bank accounts and opened credit cards in their names. The scheme centered on an employee of Teledata, a company that provides credit reports to banks and other lenders; the employee stole the passwords and codes of Teledata clients such as Ford Motor Company in order to download credit reports from the three major credit reporting agencies. Over a 10-month period, the password and code for Ford Motor Credit alone was used to download 13,000 credit reports from just one credit reporting agency, Experian. Losses were originally calculated at $2.7 million, but were expected to rise significantly in the weeks after the arrest.[1]

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

- Acxiom: In 2003, the records of an unknown number of consumers were stolen from commercial data broker Acxiom, based in Little Rock, Arkansas. Hackers were able to download the passwords of 300 business accounts on Acxiom's system, costing the company $5.8 million in losses.[2]
- ChoicePoint: In February 2005, ChoicePoint notified 144,000 consumers nationwide that their personal data may have been accessed by "unauthorized third parties" who were posing as small-business customers. ChoicePoint, an Atlanta-based data broker and specialty credit reporting agency with databases that contain 19 billion public records about consumers and businesses, reported that identity thieves created as many as 50 fake companies that posed as customers and gained access to consumer data.[3]
- Bank of America: Also in February 2005, Bank of America announced that it lost computer backup tapes containing personal information, including names and SSNs, relating to 1.2 million federal workers. The tapes had been lost two months earlier, in December 2004. Bank of America received permission from its federal regulators to notify consumers about the security problem in mid-February.[4]
- DSW Shoe Warehouse: On March 8, 2005, DSW Shoe Warehouse announced the theft of credit card information, including account numbers and customer names, relating to customers at more than 100 of its 175 stores. The theft took

[2] DOJ, Milford Man Pleads Guilty to Hacking Intrusion and Theft of Data Cost Company $5.8 Million, Dec. 18, 2003, available at http://www.usdoj.gov/criminal/cybercrime/baasPlea.htm.
[3] Sullivan, *Database giant gives access to fake firms; Choicepoint warns more than 30,000 they may be at risk*, MSNBC.com, Feb. 14, 2005, available at http://www.msnbc.msn.com/id/6969799/print/1/displaymode/1098/; ChoicePoint: More ID theft warnings, CNN/Money, Feb. 17, 2005, available at http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/.

place over a three-month period, beginning in early December 2004. DSW is a subsidiary of Retail Ventures, Inc., based in Columbus Ohio.[5]

- LexisNexis: On March 10, 2005, LexisNexis owner Reed Elsevier PLC announced that records of about 32,000 consumers were accessed and compromised when intruders used log-ins and passwords of a few legitimate customers to obtain access to a database of public records. The records included names, addresses, Social Security numbers (SSNs), and driver's license numbers. The breach occurred at Boca Raton, Florida-based Seisint, a data broker recently purchased by Reed Elsevier and integrated into LexisNexis. Seisint stores millions of personal records about consumers nationwide.[6] On April 12, 2005, LexisNexis announced that an additional 280,000 consumers nationwide had been affected by other security breaches of Seisint data over the past two years.[7]
- Boston College: In late March 2005, Boston College notified 106,000 alumni that a hacker had gained access to a computer database containing personal information about them. Officials of the college stated that they had to tell the affected alumni living in California about the theft due to California's notification

---

[4] Carrns, *Bank of America Missing Tapes with Card Data*, Wall Street Journal, Feb. 28, 2005, p. B2.
[5] *Credit Information Stolen From DSW Stores*, AP, March 8, 2005, available at http://biz.yahoo.com/ap/050308/dsw_credit_cards_4.html?printer=1; DSW Alerts Customers of Credit Card and Other Purchase Information Security Issues, DSW, March 8, 2005, available at http://www.dswshoe.com/ccpressrelease/pr/index.html.
[6] El-Rashidi, *LexisNexis Owner Reports Breach of Customer Data*, Wall Street Journal, March 10, 2005, p. A3.
[7] LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access, April 12, 2005, available at http://www.lexisnexis.com/about/releases/0789.asp.

law, and the officials therefore decided to tell alumni who live in other states, too, to help them limit their exposure to identity theft.[8]

- University of California: On April 1, 2005, University of California-Berkeley officials announced that a laptop computer containing information about 98,000 students and alumni had been stolen a month earlier. The information, including names, SSNs, and in some instances birth dates and addresses, was unencrypted, although the laptop was password-protected. This breach follows another incident at UC-Berkeley in September 2004 in which a hacker obtained the names, SSNs and other identifying information belonging to 600,000 people.[9]
- San Jose Medical Group: On April 8, 2005, the San Jose (California) Medical Group notified nearly 185,000 current and former patients that their financial and medical records might have been exposed following the theft of computers. The theft occurred after the group copied patient and financial information from its secure servers to two local PCs as part of a patient billing project and the group's year-end audit.[10]

Several conclusions can be drawn from a review of these events. Hackers and identity thieves employ both high-tech means for stealing passwords and other log-in information to access consumers' personal information, as evidenced by the LexisNexis and Acxiom breaches, as well as low-tech techniques to breach information systems, as evidenced by the ChoicePoint incidence. In addition, although the pace of disclosures

---

[8] Bank and Conkey, *New Safeguards For Your Privacy*, Wall Street Journal, March 24, 2005, p. D1.
[9] Fischer and Krupnick, *UC informs people of data security breach*, Contra Costa Times, Apr. 1, 2005, available at www.contracostatimes.com/mld/cctimes/newslocal/states/california/counties/alameda_county/cities_neighborhoods/berkeley/11284658.htm.
[10] Kawamoto, *Medical group: Data on 185,000 people was stolen*, April 8, 2005, available at http://www.nytimes.com/cnet/CNET_2100-7349_3-5660514.html.

about these breaches has accelerated over the past few months, it is safe to presume that breaches have been occurring regularly over the past several years. What has changed is not the existence of the problem, but rather the public's awareness of it.

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

On July 1, 2003, California's security breach notification laws went into effect. These laws require businesses and California public institutions to notify the public about any breach of the security of their computer information system where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[11] California's laws require that the notice be given without unreasonable delay, consistent with the legitimate needs of law enforcement, which can request a delay in notification if the notice would impede a criminal investigation of the incidence.[12] "Personal Information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data element is not encrypted:

- Social Security number.
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[13]

The California law allows a business or public institution to satisfy the notice requirement in several ways: written notice through the mail; electronic notice in

[11] Cal. Civ. Code §§ 1798.29 and 1798.82.
[12] Cal. Civ. Code § 1798.82(a) and (c); Cal. Civ. Code § 1798.29 (a) and (c).
[13] *Id.* at 1798.82(e) and 1798.29(e).

conformity with the Federal Electronic Signatures Act;[14] substitute notice through email, website publication, and major statewide news media if more than 500,000 consumers are affected; or in conformity with the business' or institution's own notification system, if it meets the timeliness requirements of the California security breach notification laws.[15]

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

III. THE EFFECT OF SECURITY BREACHES

Identity theft, already a growing problem, is likely to grow even more rapidly as a result of security breaches. The effect of these data leaks is to expose consumers to the threat of identity theft by the criminals who gain access to consumers' personal information. MSNBC has noted that in the six-week period from mid-February through early April, the rash of data heists has exposed more than two million U.S. consumers to possible identity theft.[16]

Current estimates of the incidence of identity theft in the United States are disturbingly high. According to a survey released in January 2005 by Javelin Strategy & Research, about 9.3 million U.S. adults were victims of identity theft between October 2003 and September 2004.[17]

Even though the vast majority of victims of identity theft do not report the crime to law enforcement authorities or credit bureaus,[18] the reported incidence of identity theft

---

[14] 15 U.S.C.A. § 7001.
[15] Cal. Civ. Code § 1798.82(g) and (h); Ca. Civ. Code § 1798.29 (g) and (h).
[16] Sullivan, *Is your personal data next? Rash of data heists points to fundamental ID theft problem*, MSNBC, Apr. 4, 2005.
[17] Saranow and Leiber, *Freezing Out Identity Theft*, Wall Street Journal, March 15, 2005, p. D1.
[18] Synovate, Federal Trade Commission – Identity Theft Survey Report, Sept. 2003, p. 9, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf. Only about 25% of all victims report the crime to local

has grown dramatically. The Federal Trade Commission reported in February 2005 that the number of identity theft complaints submitted to its Consumer Sentinel database has grown from 161,896 in 2002 to 246,570 in 2004,[19] representing a growth rate of more than 50% in two years. Victims' information is misused to perpetrate financial fraud in the vast majority of cases: fraud involving credit cards, checking and savings accounts, and electronic funds transfers represented 46% of the complaints in 2004.[20] Members of this Committee represent states that contain areas suffering the most from the growing incidence of identity theft. Out of the 50 Metropolitan Statistical Areas that have generated the greatest number of complaints relative to population, six are in California, four are in Texas, three are in each of New York, Ohio, Pennsylvania, and Wisconsin, and two are in Illinois.[21] Arizona victims of identity theft have filed the largest number of complaints relative to population, followed by Nevada, California, Texas, Colorado, Florida, New York, Washington, Oregon, and Illinois.[22]

Identity theft has a deeply negative impact on our nation's economy. According to a survey published by the Federal Trade Commission in September 2003, the total cost of identity theft approaches $50 billion per year, with victims bearing about $5 billion of the losses, and businesses bearing the remaining $45 billion. [23] The average loss from the misuse of a victim's personal information is $4,800, but for victims who had new credit card and other accounts opened in their name, the average loss is

---

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

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

[20] *Id.* at. p. 10.

[21] *Id.* at p. 13.

[22] *Id.* at p. 14.

[23] Synovate, Federal Trade Commission – Identity Theft Survey Report, Sept. 2003, p. 6.

$10,200.[24] Overall, victims spent almost 300 million hours resolving problems relating to identity theft in one year, with almost two-thirds of this time – 194 million hours – spent by victims who had new credit card and other accounts opened in their name.[25]

IV. CONSUMERS' AND STATE OFFICIALS' CONCERNS ABOUT SECURITY BREACHES

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

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

The citizens of California have received notice of security breaches as a result of that state's innovative law. Consumers in the remaining 49 states, the District of Columbia and the territories want the same right to receive notice when their personal information is accessed in an unauthorized manner. Unfortunately, in the absence of other state laws or a federal minimum standard, consumers in the other states have not consistently received notices in the recent spate of incidences. LexisNexis sent notices on a voluntary basis to affected consumers nationwide. ChoicePoint originally sent notices only to California residents; only after receiving letters from the Attorneys General of numerous states did ChoicePoint expand its notification process to include potentially affected consumers in all states.[26]

---

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

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

Rapid and effective notice of a security breach is an important first step to limiting the extent of harm that may be caused by identity theft. The Federal Trade Commission reports that the overall cost of an incident of identity theft, as well as the harm to the victims, are significantly smaller if the misuse of the victim's personal information is discovered quickly.[27] For example, when the misuse was discovered within five months of its onset, the value of the damage was less than $5,000 in 82% of the cases. When victims did not discover the misuse for six months or more, the thief obtained $5,000 or more in 44% of the cases. In addition, new accounts were opened in less than ten percent of the cases when it took victims less than a month to discover that their information was being misused, while new accounts were opened in 45 percent of cases when six months or more elapsed before the misuse was discovered.[28]

[27] Synovate, Federal Trade Commission – Identity Theft Survey Report, Sept. 2003, p. 8.
[28] *Id.*

To ensure that citizens across the nation receive adequate notice about security breaches, twenty-eight states are currently considering legislation modeled on California's law.[29]

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

The 2003 amendments to the federal Fair Credit Reporting Act[30] gave consumers the right to receive a free copy of their credit report once every 12 months, following the example previously set by seven states that require credit reporting agencies to provide free reports to their citizens.[31] However, because the FTC allowed the nationwide credit reporting agencies to stagger the implementation of the national free credit report, consumers in the Southern states — Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas — are not able to order their free reports under federal law until June 1, 2005. And consumers in the Eastern states — Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Vermont, Virginia, and West Virginia, as well as the District of Columbia, Puerto Rico, and all U.S. territories — are not able to order their free reports under

[29] According to the National Conference of State Legislatures, the following states are considering "breach of information" legislation: Alaska, Arizona, Arkansas, Colorado, Georgia, Florida, Illinois, Indiana, Maryland, Michigan, Minnesota, Missouri, Montana, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Washington, and West Virginia. *See* 2005 Breach of Information Legislation, National Conference of State Legislatures, April 1, 2005, available at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm. In addition, Massachusetts in also considering a security breach bill. *See e.g.*, Mass. S.B. 184 (2005).
[30] Pub. L. No. 108-159 (2003).
[31] *See* 15 U.S.C.A. §1681t(b)(4), grandfathering in the state provisions allowing free reports in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and Vermont.

federal law until September 1, 2005.[32] As a result, many citizens have been unable to see their credit report for free during this time of heightened anxiety over possible identity theft, causing great frustration in the Eastern and Southern states.

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

- Consumers Want to Control Access to Their Credit Reports so that Identity Theft Does Not Occur.

The 2003 amendments to the federal Fair Credit Reporting Act also gave consumers the right to place a "fraud alert" on their credit reports for at least 90 days, with extended alerts lasting for up to seven years in cases where identity theft occurs.[33] Yet many states are considering enacting stronger measures to assist consumers in combating the rapidly escalating outbreak of security breaches.[34] Two states, California and Texas, allow consumers to place a "security freeze" on their credit report. A security freeze allows consumers to control who will receive a copy of their credit report, thus making it nearly impossible for criminals to use stolen information to open an

[32] *See* Fact for Consumers: Your Access to Free Credit Reports, FTC, available at http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.
[33] *See* 15 U.S.C.A. § 1681c-1.
[34] *See* Saranow and Lieber, *Freezing out Identity Theft*, Wall Street Journal, March 15, 2005, p. D1.

account in the consumers' name.[35] Security freeze provisions will become effective on July 1, 2005, in two additional states, Louisiana and Vermont.[36] Although the credit bureaus argue that security freezes are overkill, and cause consumers more harm than good, many members of the business community in Vermont supported implementation of our security freeze law, enacted last year. Overall, consumer advocates and many State Attorneys General believe that security freeze laws are one of the most effective tools available to stop the harm that can result from data heists. Twenty states are currently considering security freeze bills.[37]

V. RECOMMENDATIONS ON ADDRESSING THE PROBLEM OF SECURITY BREACHES

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

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

---

[35] *See* Cal. Civ. Code 1785.11.2 (California); V.T.C.A., Bus.& C. 20.034 (Texas).
[36] *See* LSA-R.S. 9:3571.1 (Louisiana); 9 V.S.A. 2480b (Vermont).
[37] According to the National Conference of State Legislators, the following states are considering security freeze legislation: Colorado, Connecticut, Hawaii, Illinois, Indiana, Kansas, Kentucky, Maine, Maryland, Missouri, Nevada, New Jersey, New Mexico, New York, Oregon, Pennsylvania, South Carolina, Utah, and Washington. *See* Consumer Report Security Freeze Legislation 2005 Session, National Conference of State Legislators, March 8, 2005, available at http://www.ncsl.org/programs/banking/SecurityFreeze_2005.htm. In addition, Massachusetts is considering a security freeze bill. *See e.g.*, Mass. S.B. 184 (2005).

2. Enact a Federal Program for Regulation of Data Brokers: Enact a federal law to regulate data brokers in a manner similar to regulation of credit reporting agencies. Currently, the regulation of data brokers comes under a scattered mixture of federal laws, including the federal Fair Credit Reporting Act, the Gramm-Leach-Bliley Act (GLBA),[38] and a few other laws, and arguably these laws do not cover all the practices of data brokers. In developing a unified federal regulatory scheme for data brokers, only preempt state laws to the extent that they are less protective of consumers.

3. Strengthen the "Safeguards Rules": Enact a federal law that will strengthen the GLBA Safeguards Rules issued by the federal financial regulators and the Federal Trade Commission.[39] Currently, these rules require the covered institutions to develop a written information security plan that describes their programs to protect customer information, and to maintain reasonable security for customer information. The rules were intended to provide flexibility to account for each covered institution's size, complexity, scope of activities, and sensitivity of information handled. However, in light of the recent wave of security breaches, we believe that more definitive minimum standards of information security should be required, and that the Safeguards Rules should be expanded to more clearly cover data brokers.

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

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

4. Recognize the Important Role Of State Legislative and Investigative Efforts: States are providing key additional protections for consumers. California's security breach notification law, and the security freeze laws in California, Louisiana, Texas, and Vermont, are important examples of the critical role played by states in developing innovative solutions to the complex problems presented by data breaches. In addition, State Attorneys General and local law enforcement are playing critical roles in the investigations surrounding security breaches that have been disclosed to date. State and local law enforcement officials are cooperating with their federal counterparts to investigate and prosecute the perpetrators, and to determine if there were defects in security systems that may have allowed the breaches to occur. Congress should recognize these vital functions provided by state and local authorities, and ensure that these functions are not preempted.

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

Testimony By
Chris Swecker
Assistant Director, Criminal Investigative Division
Federal Bureau of Investigation
Before the
Senate Judiciary Committee
April 13, 2005

"Securing Electronic Personal Data:
Striking a Balance Between
Privacy and Commercial and Governmental Use."

Good morning Mr. Chairman and members of the Committee. I want to thank you for the opportunity to testify before you today about the FBI's efforts to combat Identity Theft, as well as the FBI's use of public source data.

The FBI views identity theft as a significant and growing crime problem, especially as it relates to the theft of consumer information from large wholesale data companies.

The FBI opened 1,081 investigations related to identity theft in fiscal 2003 and 889 in fiscal 2004. That number is expected to increase as identity thieves become more sophisticated and as the technique is further embraced by large criminal organizations, placing more identity theft crime within FBI investigative priorities. At present, the FBI has over 1,600 active investigations involving some aspect of identity theft. These cases are tracked utilizing a crime problem indicator code.

The FBI does not specifically track identity theft convictions and indictments, as identity theft crosses all program lines and is usually perpetrated to facilitate other crimes such as credit card fraud, check fraud, mortgage fraud, and health care fraud.

Armed with a person's identifying information, an identity thief can open new accounts in the name of a victim, borrow funds in the victim's name, or take over and withdraw funds from existing accounts of the victim, such as their checking account or their home equity line of credit.

Although by far the most prevalent, these financial crimes are not the only criminal uses of identity theft information, which can even include evading detection by law enforcement in the commission of violent crimes. Identity theft takes many forms, but generally includes the acquiring of an individual's personal information such as Social Security number, date of birth, mother's maiden name, account numbers, address, etc., for use in criminal activities such as obtaining unauthorized credit and/or bank accounts for fraudulent means.

Identity theft has emerged as one of the dominant white collar crime problems of the 21st Century. Estimates vary regarding the true impact of the problem, but agreement exists that it is pervasive and growing. In addition to the significant harm caused to the monetary victims of the frauds, often providers of financial, governmental or other services, the individual victim of the identity theft may experience a severe loss in their ability to utilize their credit and their financial identity. This loss can be short in duration, or may extend for years. It may result in the inability to cash checks, obtain credit, purchase a home or, in the most insidious cases, the arrest of the individual for crimes committed by the identity thief.

A May 2003 survey, commissioned by the Federal Trade Commission (FTC) estimated the number of consumer victims of identity theft over the year prior to the survey at 4.6% of the population of U.S. consumers over the age of 18, or 9.91 million individuals with losses totaling $52.6 billion. However, over half of these victims experienced only the take-over of existing credit cards which is generally not considered identity theft. New account frauds, more generally considered to be identity theft, were estimated to have victimized 3.23 million consumers and to have resulted in losses of $36.7 billion.

The FBI's Cyber Division also investigates instances of identity theft which occur over

the Internet, or through computer intrusions by hackers.

In recognition of this fact, and the overriding need to gather the most complete and accurate intelligence as quickly as possible the FBI has focused its efforts on developing joint investigative initiatives with our partners in law enforcement, as well as key Internet E-commerce stake holders. These initiatives have targeted escalating cyber crimes, both domestically and internationally, and invariably included numerous incidents which could be characterized as Identity Theft.

The Internet Crime Complaint Center, otherwise known as IC3, is a joint project between the FBI and the National White Collar Crime Center. This joint collaboration serves as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 receives on average more than 17,000 complaints every month from consumers alone and additionally receives a growing volume of referrals from key E-commerce stakeholders. Of the more than 400,000 complaints referred to the IC3 since its opening in May of 2000, more than 100,000 were either characterized as Identity Theft, or involved conduct that could be characterized as Identity Theft.

It should be noted that Identity Theft in its many forms is a growing problem and is manifested in many ways, including large scale intrusions into third party credit card processors, theft from the mails of printed checks, pre-approved credit card offers and mortgage documents, credit card skimming, Phishing schemes, and telephone and bank frauds, much of which is perpetrated through the use of SPAM e-mail.

The FBI is developing cooperative efforts to address the identity theft crime problem. In cities such as Detroit, Chicago, Memphis and Mobile, task forces are currently operating in

conjunction with other federal, state and local authorities as well as with affected merchants. In cities such as Tampa, San Diego and Philadelphia, efforts are underway to create or expand identity theft working groups and task forces. In addition, the FBI is focusing analytical resources on identity theft, working with other agencies, such as the FTC, to obtain identity theft data and utilize it to proactively identify and target organized criminal groups and enterprises.

Computer intrusions, or hackers, can significantly contribute to the impact and scope of Identity Theft.

Breaches of security at large providers of public source data have recently highlighted the ability of criminals to exploit the availability of data.

- In September 2004, Phillip A. Cummings pled guilty in U.S. District Court, Southern District of New York, to charges related to his role in the theft of over 30,000 consumer credit histories from 2000 to 2002.

  Cummings was an employee of Teledata Communications, Inc. (TCI) which provided customers with computerized access to the three major commercial credit bureaus: Equifax, Experian, and Trans Union. Cummings had access to confidential passwords and subscriber codes and used the information to download consumer credit histories which he then sold to several individuals, some of whom used the information to obtain credit cards and merchandise. Losses to financial institutions in this case exceeded $11 million.

  Cummings was sentenced to 14 years in federal prison and ordered to forfeit $1 million in illegal proceeds. This investigation was worked jointly with the United States Postal Inspection Service.

- In January 2003, a counterfeit check ring utilizing the identity of Richard Johnson and the company name NEXTEL (with no connection to the real corporation of that name) opened an account with ChoicePoint. Utilizing stolen names and social security numbers, the ring utilized ChoicePoint to obtain over 100 credit reports for those identities. Derrick Grayson and Robert Stewart, the leaders of that ring, and nine others, have been convicted of crimes in connection with the counterfeit check ring. Grayson was sentenced to 130 months in prison based on his cooperation in the investigation. Stewart was sentenced to 190 months imprisonment.
- On 09/01/2004, **Richard Burley and others** were charged in U.S. District Court, Eastern District of Michigan, on bank fraud and conspiracy charges for their alleged roles in an identity theft ring which derived profits of more than $2 million. This indictment was the result of the investigative efforts of the Detroit Metro Identity Fraud Task Force (DMIFTF). The DMIFTF comprises agents from the FBI, U.S. Postal Inspection Service, United States Secret Service, the Michigan State Police, and several local police departments. Since its inception in 1999, the DMIFTF has accounted for more than 100 convictions for identity theft- related crimes.
- In October 2004, ChoicePoint detected fraudulent activity in several small business accounts based in the Los Angeles, California area. In coordination with the Los Angeles Sheriff's Department (LASD), ChoicePoint arranged a controlled delivery of documents. During the controlled delivery, Olatunji Oluwatosin was arrested. The investigation determined that Oluwatosin was associated with at least 23 ChoicePoint

customer accounts. Oluwatosin has pled guilty to the charges and has been sentenced to 16 months in prison. Investigation related to this activity is ongoing. The investigations stemming from these customer accounts are assigned to a Los Angeles County Sheriff's Deputy and a U.S. Postal Inspector who are members of the Identity Theft Task Force sponsored by their respective agencies and of which the FBI's Los Angeles Field Office is a member. The FBI SA assigned to the Identity Theft Task Force has not been tasked with this particular investigation.

These breaches illustrate the ability of criminals to obtain the type of access to these data providers which is normally reserved for clients with legitimate business purposes for the use of the information. It is important to note that these represent a failure of the customer intake and authentication systems of the data providers, rather than a failure of the security of the data networks. In other words, these criminals were not permitted to access data in a manner that is inconsistent with that which is afforded legitimate businesses on a daily basis.

InfraGard is an FBI program that began in the Cleveland Field Office in 1996 as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. Today InfraGard has expanded to all FBI Field Offices with approximately 15,000 members ranging from representatives of Fortune 500 Companies to the owners of small Internet Service Providers. The membership represents a cross-section of the nation's critical infrastructures: Agriculture, Banking and Finance, Chemical Industry, College and Universities, Defense Industrial Base, Emergency Services, Energy, Food, Government, Postal and Shipping, Public Health, Information and Technology, Telecommunications,

Transportation, and the Water Supply.

At its most basic level, InfraGard is a cooperative undertaking dedicated to sharing information and intelligence, to include issues involving possibly Identity Theft, derived from various FBI cyber related investigations. InfraGard provides a forum for dialogue and relationship building between policy makers, private companies, and the law enforcement community on a number of issues. Its goal is to enable a two way information flow so that the owners and operators of systems and networks can better protect themselves, and, as a result, the United States Government can better discharge its law enforcement and national security responsibilities. Information sharing is accomplished by InfraGard Chapters, which are geographically linked with FBI Field Office territories and their FBI Special Agent Coordinators.

The InfraGard membership regularly provides intelligence and referrals that assist law enforcement's efforts to identify and counter the most significant criminal and national security threats to our country's networks.

To assist in the development of the types of cases that necessitate federal treatment, the FBI is developing financial crimes intelligence related to identity theft. The FBI utilizes analysts to review information contained in suspicious activity reports, the Federal Trade Commission's Identity Theft Clearinghouse, fraud reporting to the Internet Crime Complaint Center and other sources of data to identify and target criminal organizations engaged in identity theft.

Choicepoint, like LexisNexis and the other available data resources, has become an invaluable research tool for the FBI's analytical cadre in a number of ways. Choicepoint consolidates a large number of public information sources in a single, online location for quick retrieval. Much of the information provided by Choicepoint could only be obtained historically

by making direct and sometimes in-person contact with the originating Agency. Information from Choicepoint is used to provide useful leads for analysts and investigators to follow through on and can be integral in helping to draw connections between previously segregated pieces of data. The Choicepoint information is used regularly by investigators in contributing to probable cause for search warrants, court orders and other legal documents that are executed every day by FBI Agents.

An example of how Choicepoint can and has been used in analytical research can be seen in several of its search parameters. When the FBI has initiated an investigation, Choicpoint, through name and address information, can provide social security information on search projects. Once a social security number is available, analysts can enter this information into a new search parameter. These searches will produce all names that have ever been associated with the number. Many times, the production of these aliases can be used to run additional searches, providing even more potential leads for investigators to pursue. The automation of this multiple-source data, as with similar analytical engines, has dramatically reduced the amount of time and effort needed to include or exclude information.

The Choicepoint search engines also provide the names of potential family relatives and co-habitant data for subjects and subject addresses. When used with other informational databases, including the Bureau's internal indices, potential and concrete links can be established between multiple facets of an investigation, and often assist analysts in developing links between previously unconnected investigations. As criminals and criminal organizations become more complex, need reasonable access to potential source of data and information that might afford them the opportunity to establish these types of links which are crucial to realizing the entire scope of an investigation.

Choicepoint information is not considered in a vacuum. It is one of many investigative tools which are used in law enforcement by investigators and analysts. As with any source of information, it is considered in its relation to the totality of available information. It is particularly useful in that it allows analysts to inductively and deductively develop information about subjects, their confederates, witnesses and corporations that are associated with an investigation.

Once again, I appreciate the opportunity to come before you today and share the work that the FBI has undertaken to address the problem of Identity Theft. The FBI's efforts in this arena will continue, and we will continue to keep this Committee informed of our progress in protecting America's citizens and economy.

○