AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–451

IDENTITY THEFT: RECENT DEVELOPMENTS INVOLVING THE SECURITY OF SENSITIVE CONSUMER INFORMATION

HEARINGS

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

ON

RECENT DEVELOPMENTS INVOLVING THE SECURITY OF SENSITIVE CONSUMER INFORMATION RELATING TO IDENTITY THEFT, FOCUSING ON LAWS CURRENTLY APPLICABLE TO RESELLERS OF CONSUMER INFORMATION

MARCH 10 AND 15, 2005

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.access.gpo.gov/congress/senate/senate05sh.html

U.S. GOVERNMENT PRINTING OFFICE

28–404 PDF WASHINGTON : 2006

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

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

RICHARD C. SHELBY, Alabama, *Chairman*

ROBERT F. BENNETT, Utah
WAYNE ALLARD, Colorado
MICHAEL B. ENZI, Wyoming
CHUCK HAGEL, Nebraska
RICK SANTORUM, Pennsylvania
JIM BUNNING, Kentucky
MIKE CRAPO, Idaho
JOHN E. SUNUNU, New Hampshire
ELIZABETH DOLE, North Carolina
MEL MARTINEZ, Florida

PAUL S. SARBANES, Maryland
CHRISTOPHER J. DODD, Connecticut
TIM JOHNSON, South Dakota
JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
EVAN BAYH, Indiana
THOMAS R. CARPER, Delaware
DEBBIE STABENOW, Michigan
ROBERT MENENDEZ, New Jersey

KATHLEEN L. CASEY, *Staff Director and Counsel*
STEVEN B. HARRIS, *Democratic Staff Director and Chief Counsel*
MARK OESTERLE, *Counsel*
DEAN V. SHAHINIAN, *Democratic Counsel*
JOSEPH R. KOLINSKI, *Chief Clerk and Computer Systems Administrator*
GEORGE E. WHITTLE, *Editor*

C O N T E N T S

THURSDAY, MARCH 10, 2005

	Page
Opening statement of Chairman Shelby	1
Opening statements, comments, or prepared statements of:	
Senator Corzine	2
Prepared statement	25
Senator Sarbanes	5
Senator Johnson	7
Senator Reed	12
Senator Dole	14
Prepared statement	26
Senator Schumer	14

WITNESSES

Partick Leahy, a U.S. Senator from the State of Vermont	3
Deborah Platt Majoras, Chairman, Federal Trade Commission	8
Prepared statement	27
Larry Johnson, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service	19
Prepared statement	48
Amy S. Friend, Assistant Chief Counsel, Office of the Comptroller of the Currency	22
Prepared statement	50

THURSDAY, MARCH 15, 2005

Opening statement of Chairman Shelby	1
Opening statements, comments, or prepared statements of:	
Senator Sarbanes	14
Senator Bunning	17
Senator Schumer	19
Senator Allard	22
Prepared statement	29

WITNESSES

Don McGuffey, Vice President, ChoicePoint Services, Inc.	1
Evan Hendricks, Editor and Publisher, Privacy Times	4
Prepared statement	29
Barbara Desoer, Global Technology, Service and Fulfillment Executive, Bank of America	7
Prepared statement	34

IDENTITY THEFT: RECENT DEVELOPMENTS INVOLVING THE SECURITY OF SENSITIVE CONSUMER INFORMATION

THURSDAY, MARCH 10, 2005

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 2:50 p.m., in room SD–538, Dirksen Senate Office Building, Senator Richard C. Shelby (Chairman of the Committee) presiding.

OPENING STATEMENT OF CHAIRMAN RICHARD C. SHELBY

Chairman SHELBY. The hearing will come to order.

This afternoon we are going to hold the first of two hearings to examine the level of security that has been provided to sensitive financial information. While two incidents have received significant media attention and brought this issue to the forefront, I want to make clear that these events are only a small part of larger developments and note that I feel this overall subject requires broad, not simply anecdotal, consideration.

The fact is, technology has profoundly changed our economy. Automation, depersonalized transactions, and the electronic storage, manipulation, and transfer of massive amounts of sensitive information are entirely routine. While there are significant benefits associated with these developments, we must also recognize that there are some significant risks associated with them as well.

Most notably our rapid-fire, credit-in-a-moment economy provides tremendous opportunities for fraud and identity theft. If a crook gets hold of someone's personal information such as their name, date of birth, and Social Security number they can steal millions of dollars and wreak havoc on that person's life and credit history in only a matter of moments. For this reason, I believe it is paramount that this kind of sensitive information be properly protected.

In the past, much of the focus regarding identity theft prevention has been directed on what an individual can do to protect themselves. This was and remains very important, but identity theft criminals have grown more sophisticated and are more aggressively pursuing information from centralized data sources. At a minimum, recent events indicate that we must remain constantly vigilant regarding the financial information, security practices and entities that hold millions, if not billions, of financial records.

Thus, the purpose of today's hearing is to gain insight into the state of the industry compliance with the laws designed to protect

personal financial information and to learn whether the current legal framework provides adequate protections and has kept pace with the change in the marketplace.

We look forward to hearing from the witnesses today.

Senator Corzine, do you have an opening statement?

STATEMENT OF SENATOR JON S. CORZINE

Senator CORZINE. Yes, I do, sir. Thank you, Mr. Chairman, and I want to thank you for holding this hearing on identify theft and related security issues with regard to sensitive consumer information. I want to say your response to this emerging problem is typical of your leadership. I think it is strong leadership on a whole series of issues as has been the case with Ranking Member Sarbanes as well. I appreciate it and I know the public will because it is something of great concern.

The importance of this, as we have all heard, has been underscored recently. As the Chairman said, it may be anecdotal but it seems to be more broad based than just the occasional anecdote. Just yesterday, the announced breach of LexisNexis, the scandal at data broker ChoicePoint, and the loss by Bank of America of sensitive information on over one million individuals, among them Members of the U.S. Senate, including some sitting at this table.

These alarming instances are a stark reminder of just how vulnerable consumers and each of us are at having our personal information fall into the wrong hands, the hands of thieves. Personal information such as our Social Security numbers, drivers license, auto registration numbers, credit histories, and credit card numbers are vulnerable to people who know how to use technology for ill-begotten ways.

As alarming as the brashness of the identity thieves and the growth of the crime is, is the notion that there are likely other instances of large-scale identity theft that we have never been able to define or disclose to the public.

Mr. Chairman, identity theft is on the rise and is probably our fastest-growing consumer crime. According to the FTC, nearly 10 million Americans were the victims of identity theft in 2003, three times the number of victims just 3 years before that. Research shows that there are as many as 13 identity thefts every minute.

It is a crime that harms our economy in the form of lost productivity and capital. Aggregate estimates of the costs are not truly identified, and I think that actually identifies a problem in and of itself in the sense that we do not have a complete handle on what its impact is on the public. According to the Identity Theft Resource Center, identity theft victims spend nearly 600 working hours recovering from the crime, and the cost in lost wages can be as much as $16,000 per incident before the loss itself, and the emotional distress is immeasurable.

Technological innovation has brought about a data revolution that most consumers have benefited from, but it has come with some cost.

In this context, Mr. Chairman, next week I will be offering and introducing the Identity Theft Prevention and Victim Notification and Assistance Act. The bill takes a comprehensive approach to the problem of identity theft, better oversight, strong standards aimed

at preventing identity theft, victim notification and assistance, and tough enforcement by Federal regulators, including those that will testify today if we can give them the resources to do their job.

It authorizes the FTC to write rules requiring firms to ensure the accuracy, security, and integrity of sensitive personnel information, enhances identity theft prevention by requiring all companies maintain sensitive personal information, establish security systems that safeguard their information. I could go through the details of it, but I will submit that in a longer statement for the record. But one of the things it does is not unlike what is in Sarbanes-Oxley. It requires that the chief enforcement officer attest to the effectiveness of the systems that provide for control of information.

So there is a whole series of additional steps which I think are absolutely vital, including—and the last one might be most important—immediate notification of the consumers who are impacted by this. Too often as we saw in the ChoicePoint and other situations, people were not informed immediately. They only find out when someone has used their credit or has stolen from them, and it is a problem that needs to be addressed.

I look forward to working with the Committee, the Chairman, and my colleagues on addressing this as we go forward. Thank you very much. I have a more extensive statement.

Chairman SHELBY. Your entire statement will be made part of the record in its entirety, Senator Corzine.

Chairman SHELBY. Our first panel we have our colleague, Senator Patrick Leahy, U.S. Senator from Vermont, someone who spent a lot of time—former Chairman of the Judiciary Committee and now ranking Democrat—there in this area.

Senator Leahy, welcome to the Banking Committee. Your entire statement will be made part of the record. You proceed as you wish.

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

Senator LEAHY. Thank you, Mr. Chairman, and I appreciate the courtesy of having me here. I spoke to earlier in private about this. I will state publicly that I applaud your decision to hold today's hearing about recent security breaches at ChoicePoint and Bank of America, and what that means about protecting sensitive consumer data. You and Senator Sarbanes have been leaders on these issues and I thank you for this opportunity.

We are in a challenging area. The advanced technologies have opened up new possibilities. They have brought enormous benefits to consumers and commerce, law enforcement, and there is no doubt these advances have made our lives better, safer, but they have also created new vulnerabilities for our privacy and for our security. It is becoming increasingly clear these trends have challenged the privacy laws we currently have. And today's security saturated environment is fostering partnerships between Government and private data brokers, creating new challenges for maintaining privacy standards over the sensitive information that more and more involves every single American.

The troubling events at ChoicePoint, Bank of America, and now LexisNexis are a window on some of these weaknesses.

ChoicePoint's bread and butter business includes identity verification and screening to help corporate America, as they say, "know its customers." Well, this company failed to know its own customers. They sold personal information on at least 145,000 Americans to criminals posing as legitimate companies. It was an irresponsible violation of the fiduciary relationship they have to their customers.

Then there is Bank of America which recently announced that the personal information of more than a million Government employees, including some Senators and Senate staff members, was compromised when backup tapes disappeared during transport on a commercial airliner. We now understand this type of transport is routine not only for them but also the entire industry.

I do not know what these people are thinking. Mr. Chairman, you and I travel commercially. We travel a lot. We have had our suitcases lost. Do they think that the suitcase full of some of the most important data on their customers could not get lost too? Can you imagine how disillusioned their customers must feel when they find Bank of America did not care any more about them than to let that happen? On the eve of this hearing we have also learned that personal information on 32,000 more Americans was potentially compromised at a subsidiary of LexisNexis.

The susceptibility of our most personal data to relatively unsophisticated scams or logistical mishaps is greatly disturbing, and that is even before we consider the dangers posed by insiders, by hackers, by organized crime, and now we know by terrorists. In an era where personal information is a key commodity, the personal information of Americans has become a treasure trove, valuable but also vulnerable.

Today, companies around the world routinely traffic in billions of personal records about consumers. The magnitude of these transactions has rendered the individuals behind the data faceless. But at the end of the day if things go south, it is the consumer that bears the brunt of the harm, not the company. For consumers, caught up in the endless cycle of watching their credit unravel, and doing the damage caused by such breaches becomes life-consuming and monumental.

Congress needs to act. We have to do it right. Many of us have been examining the information brokering industry. Consumers should know who has their data, what it is being used for, how they can correct mistakes. They should have notice consistent with law enforcement considerations so they can protect themselves. That is just basic fairness.

We have to look closely at ensuring a standard of care consistent with the high value of this data, including penalty options when companies fall short of meeting those standards. Data brokers are increasingly partnering with the Government in law enforcement and homeland security efforts. It could prove useful for us here in Congress to consider the extent to which a company's privacy and security practices are the qualifying factors in securing Federal contracts, because then we could also ask what would be the appropriate penalties in the contract procurement process for any failure. So, I welcome the opportunity to work with you, with my colleagues

on Judiciary, and with this Committee. And Judiciary will also have hearings. Senator Specter and I intend to.

Privacy and liberty are important values to the American people. It is not a Democratic or Republican issue, it is an American issue. Our collective vigilance in protecting these cherished values has allowed us to enjoy unparalleled freedom, security, and economic vitality. We have to continue this vigilance.

I applaud you, Mr. Chairman. Your hearing today is going to shed much needed light on a rapidly growing industry and its practices in handling the financial and personal information of every American. I look forward to continuing to work with you. I think at the end of the day when we finish the hearings here and in Judiciary, the American people should end up being better protected, but I think they are also going to have a better idea what happens to their personal information.

Thank you, sir.

Chairman SHELBY. Thank you, Senator. We look forward to working with you and also the Judiciary and other Committees, whatever we have to do to try to secure the American people's financial information.

We have got a vote on the floor now of the Schumer Amendment. We are going to take a break and go vote, and then we will get in the second panel. We will be in recess until we get back.

[Recess.]

STATEMENT OF SENATOR PAUL S. SARBANES

Senator SARBANES. [Presiding.] First of all, let me assure you this is not a coup.

[Laughter.]

I saw Chairman Shelby in the hallway, and he is on his way for this vote, and I had just finished it. There is another vote that will be coming so we are trying to keep the process moving ahead, although it is under rather difficult circumstances. So, I am going to go ahead now and make my opening statement so we get that behind us in terms of the business yet to be done.

First of all, I want to commend Chairman Shelby for holding this very timely hearing. I underscore his quick response to the news of recent breaches of data security that potentially affect millions of Americans. Data security and financial privacy are important values in our society. They have been the subject of Banking Committee hearings and legislative markups since the 105th Congress. Title V of the Gramm-Leach-Bliley Act of 1999 contained data security and privacy protections. And the identity theft and affiliate sharing protections were in the Fair and Accurate Credit Transaction Act of 2003. Both of those bills came out of this Committee.

Security breaches, very regrettably, have led to the improper release of the sensitive personal data of millions of Americans. Last month, ChoicePoint, a data broker, described by a journalist as the world's largest private intelligence operation, sold information that had personally identifiable data on 145,000 people to imposters, people not properly entitled to the information. According to ChoicePoint's testimony, this included "access [to] information products primarily containing the following information: Consumer names, current and former addresses, Social Security numbers,

drivers license numbers, certain other public record information such as bankruptcies, liens and judgments, and in certain cases credit reports."

Bank of America, one of the world's largest financial institutions, serving 33 million consumer relationships, reported the loss of backup computer tapes which, according to testimony today, "contained customer and account information for approximately 1.2 million Government charge holders . . and may have included name, address, account number and Social Security number." I understand that both of these companies are taking actions to prevent future problems.

More data security breaches were revealed this week. On Tuesday, DSW Shoe Warehouse stores reported that credit card information from customers of more than 100 of its stores had been stolen. On Wednesday, LexisNexis announced the theft of the names, addresses, Social Security numbers, and drivers license numbers of more than 30,000 people from its Seisint subsidiary.

These and other breachers have caused widespread concern among the public and in the Congress. *The Washington Post* reported, "public ire is intensifying." I can vouch for that on the basis of the constituents who have contacted me, and I hear the same from my colleagues. We know that Americans have strong concerns about protecting their personal information. *The Baltimore Sun,* in an editorial entitled "Stealing by the Numbers," said, This is an industry ripe for Federal and State controls."

Congressional hearings are being planned and legislation is being introduced by Senator Corzine and by others to address this problem.

I strongly share the concern about the improper release of personally identifiable financial information. A particular danger is that citizens whose data is compromised may become victims of identity theft, which is of course a serious national problem that has grown in recent years. Honest citizens who become identity theft victims incur a high cost in money, time, anxiety, and efforts to correct their spoiled credit histories and restore their good credit name. While swift apprehension and punishment of criminals is important, we must also seek to prevent breaches, to enable consumers to protect themselves, and to assist citizens who have become victims through no fault of their own.

Many questions are raised. What potentials harms to consumers can result from breaches of personal data held by financial institutions or data brokers? How are the data practices of data brokers and financial institutions regulated? What steps should be taken to prevent future breaches? Is additional Federal regulation needed in order to adequately protect consumers? Should consumers be given more rights to protect data about themselves, giving consumers the rights to have access to a copy of the records and to correct errors, or requiring notification of consumers when data breaches occur? And should financial institutions more fully inform consumers about the specific types of information they possess and what they do with data?

Other questions also of course occur, and I expect this to be a matter which the Congress will examine very carefully.

Do you have a statement, Senator Johnson?

STATEMENT BY SENATOR TIM JOHNSON

Senator JOHNSON. Yes, thank you, Senator Sarbanes. I appreciate both you and Chairman Shelby for convening this important hearing, and I welcome the distinguished panel of participants that we have here today. I regret that we have these ongoing votes plus a markup in the Budget Committee, which is going to take me away from being here personally, as much as I would like to be. But it is my hope that this is just the first of a series of hearings about information security. Clearly, we need to take a hard look at whether governing statutes are adequate to protect the increasing body of personal information databases. I appreciate the clarity with which the FTC has summarized those laws in its written testimony, and I hope that we can work together to legislate in a speedy and effective manner to capture all industry players.

Mr. Chairman, I believe that we also need to take a close look at what we can do within the current legal framework to protect sensitive personal and financial information. We know companies face significant and ongoing problems with both insider breaches and outside hackers. In these cases, the problem is not the absence of a governing statute, but rather a violation of an ongoing statute.

I would like to call the Committee's attention to some innovations in the area of data security which bear discussion. One example is Dakota State University in Madison, South Dakota. DSU's Information Assurance program has developed important technologies to protect community banks from information breaches. DSU recently won accreditation from the National Security Agency for its bank-focused program which specializes in assisting banks to protect sensitive information within current legal frameworks.

A security breach is costly both financially and toward reputation. Many companies, though regrettably not all, go beyond legal requirements to ensure the security of their data. I hope through this hearing process we will get a better sense of the landscape of technologies available to financial and other institutions that might help them protect their databases.

As we examine how to capture all players with access to sensitive financial and personal information in a regulatory framework, we need to be careful to preserve the success of the Fair Credit Reporting Act. I was struck just this past week again by the potential benefits that FCRA can bring consumers who handle credit responsibly.

As we stand poised to pass bankruptcy reform legislation, I believe that the credit reporting system may be able to play a positive role in helping bankruptcy filers rehabilitate their credit more quickly.

In the coming weeks, it is my intention to work actively with the bankruptcy advisory committees and trustees, the credit bureaus, and the industry players to encourage a full reporting of Chapter 13 payment plans to credit bureaus. The credit reporting system is only as good as the information contained in it, and we have an important opportunity to encourage reporting that will help hard-working Americans who have fallen on hard times prove that they can in fact handle credit responsibly. Those people who are able to repay any part of their debt should get credit for that effort, and I intend to work hard to make sure that that in fact happens.

Thank you, Senator Sarbanes.

Senator SARBANES. Thank you very much, Senator Johnson.

I think the best course now would be to recess again because there is a vote about to happen, and I think the Chairman will then be on his way back, and I think he will then be in a position to go into the hearing with the next panel, which I gather would be with the Chairwoman of the FTC.

Thank you all very much.

[Recess.]

Chairman SHELBY. [Presiding.] The Committee will come back to order. We are sorry about the inconvenience, but that is the way the Senate works, two straight votes.

Our second panel we have the Chairman of the Federal Trade Commission, Deborah Platt Majoras. We welcome you to the Committee. Your written statement will be made part of the record in its entirety. You proceed as you wish.

STATEMENT OF DEBORAH PLATT MAJORAS
CHAIRMAN, FEDERAL TRADE COMMISSION

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

I am grateful for the opportunity to testify about identity theft, the security of consumer information, and in particular, the collection of that information by data brokers.

Although the views expressed in the written testimony represent the views of the entire Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or the other Commissioners.

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

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

Identify theft is a pernicious problem. A recent FTC survey estimated that as many as 10 million consumers discovered that they were victims of some form of identity theft in the 12 months preceding the survey, costing consumers nearly $5 billion in losses, and American businesses roughly $48 billion in losses. We must look seriously at ways to reduce identity theft which has shaken consumer confidence to the core.

One means of reducing identity theft is to ensure that sensitive, nonpublic information that is collected by data brokers is maintained securely.

There is no single Federal law governing the practices of data brokers. There are, however, statutes and regulations that address

the security of the information they maintain, depending on how the information was collected, and how it is used.

The Fair Credit Reporting Act, for example, makes it illegal to disseminate consumer report information, like credit reports, to someone who does not have a permissible purpose; that is, a legitimate business need for the information. Thus, data brokers are only subject to the FCRA's requirements to the extent that they provide consumer reports, as that term is defined in the statute.

Similarly, the Gramm-Leach-Bliley Act, which the Commission also enforces, imposes restrictions on the extent to which financial institutions may disclose consumer information related to financial products and services. Under Gramm-Leach-Bliley, the Commission issued a 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 companies had not taken reasonable precautions to safeguard consumer information.

Finally, in the third statutory regime, Section 5 of the FTC Act prohibits unfair and deceptive practices by a broad spectrum of businesses, including those involved in the collection or use of personal information. Under this authority, the Federal Trade Commission has brought several actions against companies that have made false promises about how they would use or secure sensitive personal information, and these cases make clear that an actual breach of security is not necessary for enforcement under Section 5 if the Commission determines the company's security procedures are not reasonable in light of the sensitivity of the information that they collect and hold. Evidence of a breach, of course, may be relevant, though, to whether the procedures were not adequate. It is important to remember, though, that there is no such thing as perfect security, and breaches can occur even when a company has taken every reasonable precaution.

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

Although data brokers are currently subject to this patchwork of laws, depending on the nature of their operations, recent events clearly raise the issue of whether these laws are sufficient to ensure the security of their information. I believe that there may be additional measures that would benefit consumers.

The most immediate need is to address the risks to the security of the information. Extending the Commission's Safeguards Rule to sensitive personal information collected by data brokers is one sensible step that could be taken. It also may be appropriate to consider a workable Federal requirement for notice to consumers when

there has been a security breach that raises a significant risk of harm to consumers.

Mr. Chairman, Members of the Committee, the FTC shares your concern for the security of consumer information, and we will continue to take steps within our authority to protect consumers. Thank you for the opportunity to discuss this vital topic, and I would be happy to respond to your questions.

Chairman SHELBY. Thank you, Madam Chairman.

The Federal Trade Commission does a lot of work that is directed at helping individuals protect themselves from identity theft. Is that correct, Madam Chair?

Ms. MAJORAS. That is correct.

Chairman SHELBY. Additionally, you also do a great deal to help individuals recover from the damage done—and this is a big thing—by identity thieves. You are clearly well aware in your position of the kind of damage that can be inflicted on the average American. We have heard horror stories here—you hear them every day, I am sure that have involved massive amounts of data involving thousands, even millions of people, recent cases. Could you provide us your views as to what kind of damage this kind of large-scale information theft can cause, just for the record?

Ms. MAJORAS. The biggest injury, of course, is identity theft on potentially a massive scale when we have a substantial security breach. The majority of the incidents that we see involve the misuse of existing accounts, but a far more destructive practice is when an identity theft takes the personal information for a particular consumer, poses as that consumer, and opens new accounts. That is one of the most difficult problems for consumers to overcome when they are trying to get their financial and personal life back, quite frankly.

Chairman SHELBY. Isn't this one of the biggest robberies going on in the country today?

Ms. MAJORAS. It is 9 to 10 million people a year, Mr. Chairman. That is 4.5 percent of our adult population.

Chairman SHELBY. And involving billions of dollars?

Ms. MAJORAS. Involving billions of dollars, not only to consumers but also to businesses, and we estimate that per year about 300 million hours of time goes into dealing with identity theft in terms of consumers trying to get their identities back and businesses, of course, trying to work through what has happened, what fraud has occurred, and what can be done to fix it.

Chairman SHELBY. Our traditional bank robbers are petty thieves compared to the aggregate of this, are they not?

Ms. MAJORAS. Some of them certainly are, Mr. Chairman, yes.

Chairman SHELBY. Could you give us several examples of the kinds of sensitive financial information that would be included in the credit report?

Ms. MAJORAS. The most common type of information would be information about consumers' accounts and, in particular, credit card accounts. So information on a credit report would include the account number, the account balance, the consumer's credit history.

Chairman SHELBY. Real private things.

Ms. MAJORAS. Very private.

Chairman SHELBY. Isn't this kind of information supposed to be covered by the protections of FCRA?

Ms. MAJORAS. The FCRA does cover this type of information, depending on how the information is used.

Chairman SHELBY. Okay.

Ms. MAJORAS. I think the easiest way to say it is to determine a consumer's eligibility for credit, for employment, for insurance purposes, then that information falls within the FCRA.

Chairman SHELBY. What kind of safeguards does the FCRA have to ensure that credit reporting agencies do not provide credit reports to anyone coming in off the street?

Ms. MAJORAS. The FCRA requires that consumer reporting agencies and anyone else who falls within the statute to have in place reasonable procedures to ensure that those to whom they sell the information have a permissible purpose, that is, an appropriate business purpose, as I said most commonly determining a consumer's eligibility for credit, for employment, or insurance.

This means under the FCRA that the CRA's must receive certification from those to whom they sell the information, and they also must make a reasonable effort to verify the user's identity and also that the user, in fact, does have a permissible purpose.

Chairman SHELBY. Ma'am, how many firms are there in the data brokerage industry? And how big is their information capacity? In other words, how much data on how many Americans are they dealing with?

Ms. MAJORAS. I am afraid that is a tough one to answer, Mr. Chairman. We have not been able to find statistics on the number of data brokers there are. We know that there is a great variety, and, of course, it depends on how you define it.

Chairman SHELBY. If you do find out something approximately the number, can you furnish that for the record?

Ms. MAJORAS. We would be pleased to present that for you, Chairman Shelby. I will say, however, that we know that individual data brokers, just like the CRA's, can have billions of pieces of data regarding consumers.

Chairman SHELBY. A treasure trove of all of the financial private information in a sense.

Ms. MAJORAS. Yes, indeed.

Chairman SHELBY. Do you think that data brokers take steps to avoid becoming credit reporting agencies to avoid the FCRA requirements? And if so, how do they accomplish this?

Ms. MAJORAS. Actually, what we have seen in the data brokerage industry is that some of the products they sell actually do fall within the FCRA and some of them do not. And it just depends on the type of products.

Chairman SHELBY. You have to look at the situation.

Ms. MAJORAS. You have to look at each individual—and, again, because it is dependent not on the label you put on the type of company, it is dependent on the kind of information, that makes a difference.

Chairman SHELBY. Sure. Do you have any information about the manner in which the Gramm-Leach-Bliley information use restrictions flow with information? In other words, could you give us a little detail about where Gramm-Leach-Bliley use restrictions flow

with information? Am I clear? In other words, these rules do not simply apply to financial institutions that have the relationship with the consumer. They apply downstream as well, do they not?

Ms. MAJORAS. They absolutely do. Once a financial institution covered by GLB provides information to a nonaffiliated party, that party is then also subject to the security provisions.

Chairman SHELBY. Give us an example, if you could, a specific example. What kind of information is covered by Gramm-Leach-Bliley?

Ms. MAJORAS. Nonpublic personal information.

Chairman SHELBY. Okay.

Ms. MAJORAS. Which the financial institutions are collecting so that they can provide financial services.

Chairman SHELBY. Proprietary information?

Ms. MAJORAS. Yes, although it is defined very broadly, so it includes name, address, Social Security number, and account numbers.

Chairman SHELBY. Things about your family?

Ms. MAJORAS. If they have it. Mother's maiden name is one that often is asked for.

Chairman SHELBY. Is this kind of information used very often by or is it very important to data brokers, all this stuff you are talking about?

Ms. MAJORAS. It is important to data brokers generally, depending on what they are selling information for. It is the information that we understand data brokers do collect.

Chairman SHELBY. Do you know if there are any meaningful safeguards that the data information brokers have to jump through before they sell information?

Ms. MAJORAS. It depends. Some of the information they provide may fall under the FCRA, and if that is the case, then they have to comply with that. If they were a financial institution or they were receiving information from a financial institution and they are a downstream reseller, then they would have some requirements under Gramm-Leach-Bliley. And, of course, we enforce Section 5 of the Federal Trade Commission Act, so we can look for deception and unfairness.

Chairman SHELBY. Is this the kind of information that is in these data banks that identity thieves would be interested in?

Ms. MAJORAS. There really is not any question. They are interested in identities of individuals that perhaps they could pose as, and they are absolutely interested in account numbers.

Chairman SHELBY. Again you said earlier in, I believe, your opening statement, was it 40-something billion dollars a year loss to businesses, and then so much to consumers, too?

Ms. MAJORAS. That is correct. So if we put our estimates for out-of-pocket losses to businesses and consumers together, it is well over $50 billion.

Chairman SHELBY. Senator Reed.

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman. Thank you, Chairman Majoras. This is a very important hearing. I am sure everyone has made that point quite clearly.

Let me ask a question. We were talking about essentially domestic operations, but there is a growing trend to outsource these types of information searches and data manipulation overseas. Does that pose another additional problem to you?

Ms. MAJORAS. Well, it may. There are some difficulties that we have generally with any kind of fraud over the Internet when it crosses more than one border, as more and more we are seeing in this Internet information age. And we have been working on legislation that would give us better tools to address cross-border fraud, and some of this would absolutely fall into that category.

Senator REED. Last year, Senator Corzine in the reauthorization of the FCRA proposed an amendment that would require prompt notification of breaches. That amendment was dropped in the conference. Would this prompt notification be useful given the experience we have just witnessed in the last few weeks?

Ms. MAJORAS. We think prompt notification when there is a significant risk to consumers is what makes the most sense. And the reason that we say that is that there are some security breaches that occur that really actually do not present harm to consumers. And there is a great cost to notifying consumers of every breach. One might have a hacker who is a teenager in someone's garage who enjoys seeing if he or she could hack into a database and might do it and then call and say, "Ha, ha, I did this," but is not stealing information. And there are other, if you will, breaches on a smaller scale.

If we try to inform consumers of every single breach, for one thing they are going to become numb to it. It will be very much, okay, all right, sure, I am at risk; and then they may not take the precautions which the FTC and others encourage them to take when there really has been a significant breach.

So we think there has to be some—that the best course is to have some limitation on it so that companies must take reasonable steps when there is a significant risk.

Senator REED. Right now, there is no requirement in Federal legislation to make this notification; is that accurate?

Ms. MAJORAS. Not quite. I know that the OCC—and I know that you will hear from one of their witnesses—has proposed guidance through their Gramm-Leach-Bliley implementation, which actually proposes a very similar requirement to the one I was just discussing, which is you would take some reasonable precautions when you think that consumers really are at risk.

Senator REED. You have alluded to legislation that you are working on with respect to international ramifications of technology and the Internet that is spreading across the globe and what you have just mentioned with respect to notification. Are there any other safeguards that you would urge us to consider with respect to problems like we have seen?

Ms. MAJORAS. I think considering taking the FTC's Safeguards Rule, which we promulgated under Gramm-Leach-Bliley, and extending it more broadly so that the requirements that we have in the safeguards will go beyond just financial institutions that are covered by GLB but, in fact, would cover more companies, which would include the data brokers.

The difficulty in passing too many statutes in which we try to limit it to particular labels that we can put on a company is that our commerce and our society, as we can see today, is changing so quickly that if we use something like the FTC Safeguards Rule, which requires companies to use reasonable precautions depending on type of company they are, the sensitivity of the data, the surrounding circumstances, is likely the best way to deal with this problem on a broader basis.

Senator REED. Thank you, Madam Chairman.

Ms. MAJORAS. You are welcome.

Chairman SHELBY. Senator Dole.

STATEMENT OF SENATOR ELIZABETH DOLE

Senator DOLE. Mr. Chairman, I ask unanimous consent that my statement go in the record, please.

Chairman SHELBY. Without objection, it is so ordered.

Senator DOLE. Madam Chairwoman, let me ask you about your testimony where you mention reasonable procedures to ensure that a credit reporting agency supply consumer reports only to those with an FCRA-sanctioned permissible purpose. Could you tell the Committee what the FTC considers to be a reasonable procedure?

Ms. MAJORAS. Fortunately, the FCRA then goes a little beyond requiring reasonable procedures and then imposes some very specific requirements. So, for example, before companies subject to the FCRA release the type of information covered by that statute, they must get certification from the user that it will be used for a permissible purpose. And they also have to take reasonable steps to verify that.

Now, those reasonable steps have included things like making on-site visits to companies to make sure that they are actually legitimate businesses who are using this information for legitimate purposes under the statute.

Senator DOLE. So this reasonable procedure standard would work well for consumers, and do you think in any way that Congress should consider strengthening it?

Ms. MAJORAS. We think it is a reasonable standard for ensuring that consumer reports are provided only to those who have a permissible purpose, and the reason is it is flexible enough to apply to all types of businesses who have this sensitive information and so that it can be tailored according to the sensitivity of the information as well. So, yes, we actually think this would be a reasonable way to proceed.

Senator DOLE. Thank you, Mr. Chairman.

Chairman SHELBY. Thank you.

Senator Schumer.

STATEMENT OF SENATOR CHARLES E. SCHUMER

Senator SCHUMER. Thank you, Mr. Chairman, and I appreciate very much your having this hearing, and I know your interest in this issue, which is mine as well, from being a Member of this Committee as well as the Judiciary Committee. And I look forward to working with you to help solve this kind of problem.

Let me say, Mr. Chairman, that identity theft costs businesses millions of dollars each year because criminals use false pretenses

to purchase goods, leaving businesses to foot the bill. Identity theft costs consumers and businesses an estimated $5 billion a year, and, in addition, the typical identity theft victim has to spend about 175 hours to clear up his or her credit report.

Identity theft is skyrocketing. Every year it gets much worse and yet we are doing very little about it. Our laws are a patchwork quilt of State and Federal laws that, frankly, do not do the job. And if we do nothing, this is going to almost envelop crime-fighting in America. It is the crime of choice these days.

What bank robbery was to the Depression Era, identity theft is to the Information Age.

My point is that we in Congress need to learn the lessons of ChoicePoint, LexisNexis, Westlaw, and so many other companies, all of whom seem to feel that your personal information was their domain to do with whatever they chose. We need to replace the current patchwork of State and Federal laws with a real security blanket, one that protects privacy, keeps Social Security numbers private, and prevent fraud and identity theft.

Right now, Mr. Chairman, there is no arm of the Federal Government that has clear jurisdiction over online and off-line identity theft. Companies seeking to obtain personal data from customers are subject to few, if any, limitations. I am utterly amazed at how companies allow anyone to get hold of this information and even let almost anyone work within them. You know, it is like not having background checks for people working at Fort Knox.

And, finally, customers have no idea if or when a company might transfer personal data to a third party. Too many consumers are entrusting their information to companies for safekeeping, only to have it sold away for the highest dollar, often in the dark of night.

We learned this even here in the Senate with Westlaw, where just about anyone on the Senate staff with no background check, interns or anybody else, could get 95 percent of all Americans' Social Security numbers. No questions asked. That was on our Senate server until we brought this to the public's attention, and now they have blocked out the last four numbers.

Mr. Chairman, we have to do something about this. We have to stop malicious companies conning consumers out of their information with privacy policies that are impossible to understand. Often all of those lines of legalese mean only one thing. You get all these pages, and what they basically are saying is we will sell your personal information to whomever we want, whenever we want. And this has to stop.

To plug these loopholes, I will be introducing comprehensive identity theft legislation in the near future which would, Mr. Chairman, create an Office of Identity Theft in the FTC to have jurisdiction over companies that lawfully acquire and keep personal consumer data. It will also create a Schumer box to be posted on any website that seeks to request personal information from a customer. In that box, companies would give a clear warning in simple language to consumers if they plan to sell their information. This is like the Schumer box that we successfully did for credit cards, and it helped bring down credit card interest rates. It was clear and simple and it was required to be published.

And, finally, we are going to force companies to demonstrate a need for customers' personal information before requiring it from them, as well as making sure that those who handle the information are carefully screened. It is high time for Congress to fill the breach that hackers, thieves, and the Internet have combined to create, leaving consumers vulnerable and costing our economy billions. Again, I want to ask my friend from Alabama, the Chairman of this Committee, who has been a thoughtful and persistent advocate for privacy—I remember this from all the banking bills we worked on together—to work with us to create a bipartisan, comprehensive piece of legislation that will really get to the heart of the information epidemic.

With that, I have a couple of questions for our witness. For years the FTC has built the expertise to address consumer issues in a variety of industry sectors. When Congress, for instance, enacted the Fair Credit Reporting Act, the FTC built on that expertise to examine abuses in the credit card industry.

Beyond the dissemination of helpful hints, which is what you have done so far, does the FTC have sufficient jurisdiction to examine identity theft allegations?

Ms. MAJORAS. Thank you, Senator Schumer. We have jurisdiction to examine some of them. Now, remember that identity theft itself is a crime, and the FTC does not have criminal jurisdiction. So that is number one.

On the civil side, however, we have authority to enforce the FCRA when the information that is being provided is subject to that statute. We have some authority over some financial institutions who are subject to Gramm-Leach-Bliley. And, of course, we have Section 5 of the FTC Act, in which we can attack deceptive or unfair conduct and which we have done in the area of information security several times recently.

Chairman SHELBY. But DSW, the store, that has thousands of lines of personal data. Do you have jurisdiction over how they handle that data, whether they can sell it, what they do with it?

Ms. MAJORAS. I have to be careful about talking about any particular company.

Senator SCHUMER. Okay. Let us take a hypothetical shoe store that kept a lot of people's data.

[Laughter.]

Ms. MAJORAS. Thank you, Senator. Under Section 5 of the FTC Act, we can take a look at security measures that companies have in place, which we already have done in some cases, and——

Senator SCHUMER. But isn't Section 5 a fraud provision?

Ms. MAJORAS. It is.

Senator SCHUMER. So let's say they attached—when you signed out to buy shoes at this hypothetical shoe store, there was something in small little language way at the back that said, hey, we can sell your information to whomever we want. They wouldn't be committing fraud. What would give you the jurisdiction?

In other words, I think the jurisdiction has to go—notification is important, but it goes beyond that in this modern world we are in.

Ms. MAJORAS. Well, and I am not suggesting, Senator, that some other tools would not be useful, both in the area of security and in the area of notice, as I said in my testimony. But we do think—

yes, it is true, the five cases we brought under the FTC Act so far have been instances in which companies have told consumers we are protecting your data and then they did not. So you are right. That was the deception we attacked.

But, in addition, it might be possible, depending on the egregiousness and the circumstances, to use the Unfairness Doctrine to attack some of these practices.

Senator SCHUMER. Right. Let us take—well, you do not want to talk about a specific case. Aren't there many instances where this hypothetical company would not really need the customer's Social Security number but would ask for the purpose of selling it?

Ms. MAJORAS. Sometimes we have seen instances where out of habit, for example, Social Security numbers are requested when they are not needed. Now, sometimes they are needed. They are used for matching. They are used for matching so that the right consumer is matched with the right information.

Senator SCHUMER. Got you. Okay. Are we making it too easy for companies to collect and disseminate this information in the first place? What is your judgment on that?

Ms. MAJORAS. I am not sure how—are we making it too easy?

Senator SCHUMER. Or is it too easy? Not are we making it. Is it too easy is a better way to ask the question.

Ms. MAJORAS. Right. Data brokers, in particular, collect information from many sources, including many publicly available sources.

Senator SCHUMER. Right.

Ms. MAJORAS. And lots of public records information. They then do get nonpublic information as well. Now, why do they get it and why do they sell it? Because there is a market need for it.

Senator SCHUMER. No question.

Ms. MAJORAS. So that is why they do it. So it is easy for them to get it. I think that what we really should be looking at is how they secure the data and making sure they secure it, because there are a lot of beneficial uses to this information, Senator, things that consumers have come to count on.

Senator SCHUMER. No one is saying that there should be no data held by anybody, and it is even a difficult question to say should you need the permission of the person. But we are the opposite. We are in the Wild, Wild West here where they can collect the information from legal and/or public and nonpublic sources. And they can use it in just about any way they choose. And we have seen just in the last month, almost every third day you see another major example of data theft, identity theft. So we clearly have to change the law. Don't you agree with that?

Ms. MAJORAS. We think that we should look at a broader security standard that is not—as you say, we have a patchwork in the law today.

Senator SCHUMER. Right.

Ms. MAJORAS. And so it depends on how this information is used and what kind of company, whether it is a financial institution and so forth. And we think if you look at the approach we have taken under Gramm-Leach-Bliley at the FTC with our Safeguards Rule, where we require companies to have reasonable procedures—and what does that mean? It means you have to look at the sensitivity of the data. You have to look at what it is used for and develop

security procedures that will protect the type of data that is being collected.

Senator SCHUMER. Was ChoicePoint under your jurisdiction under Gramm-Leach-Bliley?

Ms. MAJORAS. It depends on whether it is a financial institution.

Senator SCHUMER. I understand.

Ms. MAJORAS. And that is an issue we are looking at in the investigation.

Senator SCHUMER. Well, haven't you then answered my question?

Ms. MAJORAS. But also, as we understand it——

Senator SCHUMER. Wait, wait. Madam Chairman, if you cannot answer yes or no succinctly whether ChoicePoint, one of the most major data collection companies in the country, is under your jurisdiction or not, don't you think we need to tighten this up?

Ms. MAJORAS. I think they are potentially under three statutes, but because we are—as they have acknowledged publicly, because we are investigating them, I am just being ultra-cautious.

Senator SCHUMER. But that is a different question as to what the investigation reveals about what they did. Jurisdiction is a separate issue. Isn't the law kind of vague? I mean, in certain places under Gramm-Leach-Bliley, it is clear. A bank.

Ms. MAJORAS. Right. That is right.

Senator SCHUMER. With many of these others, it is not clear at all. And my guess is, if the company is this hypothetical shoe company, you do not have jurisdiction unless fraud comes to your attention right away. But you would not have jurisdiction barring fraud to set standards right now. Is that correct?

Ms. MAJORAS. We think it is broader than that under Section 5, Senator. But I absolutely agree with you that this is a complicated maze and that there is not one place to go to say yes, this practice, whether it is by ChoicePoint or anyone else, unless, as you say, it is bank, is absolutely subject to this statute. We are piecing together three statutes——

Senator SCHUMER. Right. So, therefore, we need some changes, correct?

Ms. MAJORAS. Security and notice, yes.

Senator SCHUMER. Yes, okay. Let us see.

Let me ask you this: Would it help consumers if companies were required to notify their customers before transferring their data to a third party? I did not specify the type of notification. It could be specific—we are giving this data to whom, or it could be in general—be careful, your data could be disseminated. Would that be a good idea, bad idea, neutral, in your opinion?

Ms. MAJORAS. It all depends on the database. There are some databases that are used to go after people who have committed fraud. And, of course, we would not want to tell them in advance we are looking at you, or personal information to try to find you because you have victimized other consumers.

Senator SCHUMER. Let us say I sign up for a loan at the bank. Would it not be a good idea to tell somebody, to tell me this information you are giving us might be disseminated to other people; we even might sell it.

Ms. MAJORAS. Yes. And for a bank, we have that under Gramm-Leach-Bliley and we have an opt-out provision.

Senator SCHUMER. Right. Exactly. And what if it is a nonbank that sells a good? Why would we not want to do that to them? It is a nonfinancial institution.

Ms. MAJORAS. Again, it just depends on what they are using the information for.

Senator SCHUMER. It is a hypothetical shoe company.

Ms. MAJORAS. Well, it is a hypothetical shoe company who is going to sell what kind of information?

Senator SCHUMER. Well, you know——

Ms. MAJORAS. I mean, most certainly, Senator, if they were going to sell credit card information, then by all means.

Senator SCHUMER. Okay, good. I was not referring to shoe size. I do not know: Give me a list of all the Size 8–D's in Kansas. I was not quite thinking of that.

Ms. MAJORAS. Well, sometimes marketing information is what we are talking about.

Senator SCHUMER. Okay. So in general, notification would be a good idea, except there would have to be outlier situations, fraud and things like that. General notification.

Ms. MAJORAS. I think there are a number of situations in which notification might not be the best course.

Senator SCHUMER. Okay. I do not want to ask you about the ChoicePoint. That is not really your jurisdiction, right, the ChoicePoint executive officers? This is more SEC, from what they did. Or are you looking into that as well?

Ms. MAJORAS. We are investigating ChoicePoint.

Senator SCHUMER. No, that I know. Okay.

I think I am finished with my questions, Mr. Chairman.

Chairman SHELBY. Thank you, Senator Schumer.

Madam Chairman, we look forward to working with you. We appreciate your appearance here today. There are some things that we might work together to tighten up in this area, and we will be awaiting your investigation.

Ms. MAJORAS. Thank you very much, Mr. Chairman. Thank you, Senator Schumer.

Chairman SHELBY. Our third panel consists of Mr. Larry Johnson, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service; Ms. Amy Friend, Assistant Chief Counsel, Office of the Comptroller of the Currency.

If you two would come to the table. Both of your written testimony will be made part of the record in its entirety.

Mr. Johnson, we will start with you. Welcome to the Committee.

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

Mr. JOHNSON. Thank you, Mr. Chairman, and Members of the Committee.

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 customers and industry from financial fraud. With the passage of the new Federal laws in 1984, the Secret Service was provided primary au-

thority for the investigation of access-device fraud, including credit card 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 times of financial crimes. Our efforts to detect, investigate, and prevent financial crimes are aggressive, innovative, and comprehensive.

The expanding use of the Internet and the advances in technology, coupled with increased investment and expansion, has intensified competition within the financial sector. With the 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 by-product of the new, 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 market, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that that information provided in credit card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. Customers may even be less aware of the legitimate uses to which this information can be utilized.

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. But legitimate businesses can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

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 by the Secret Service 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 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 deception, such as phishing, Web-spoofing, or even social engineering.

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 billing centers, financial institutions, medical offices, or Government agencies. Once the criminal has obtained the proprietary information, it can be exploited by creating false breeder documents, such as birth certificates or Social Security cards. These documents are then used to obtain genuine false identification such as driver's licenses and passports. Now the criminal is ready to use the illegally obtained personal information to apply for credit cards, consumer loans, or establish bank accounts, leading to the laundering of stolen or counterfeit checks or to conduct a check-kiting scheme.

I would like to talk a little bit, Mr. Chairman, about agency coordination. It has been the Secret Service's experience that the criminal groups involved in these types of crimes routinely operate in a multijurisdictional environment. This has created problems for law enforcement agencies that generally act as first responders to 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 crimes 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. The members of these task forces, who include representatives from State and local law enforcement, prosecutors offices, private industry, and academia, pool their resources and expertise into 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 authorizes Secret Service pursuant to the USA PATRIOT Act of 2001 to expand our electronic crimes task forces to cities and regions throughout the country.

Finally, the best example of agency cooperation came in October 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 multicount 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 the Secret Service-led investigation.

This case began in July 2003, when the Secret Service initiated an investigation involving global credit card fraud and identity fraud. Although the catalyst for the crime came from a more traditional crime of access-device fraud, the case evolved into a very technical transnational investigation. Much of the aforementioned criminal activity primarily occurred over the Internet. After the initial acts of fraud, suspects would exchange contraband, for example, counterfeit credit cards, counterfeit driver's licenses, et cetera. This case, entitled Operation Firewall, developed into a multilat-

eral 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 of a computer network.

Mr. Chairman, that concludes my oral comments.

Chairman SHELBY. Thank you.

Ms. Friend.

STATEMENT OF AMY S. FRIEND, ASSISTANT CHIEF COUNSEL, OFFICE OF THE COMPTROLLER OF THE CURRENCY

Ms. FRIEND. Thank you, Mr. Chairman.

The OCC appreciates the opportunity to testify about a subject that is essential to the integrity of the relationship between a bank and its customers—a bank's ability and legal obligation to safeguard customer information. We commend the Committee's leadership in addressing this important subject.

It is a matter of primary importance to the OCC, as it is to the Committee, that national banks have adequate procedures in place to safeguard customer information. Safeguarding customer information is critical to protecting consumers and maintaining the safe and sound operations of a bank. For that reason, information security has been a part of our overall exam process for years.

More recently, the OCC has been examining for and enforcing compliance with the information security guidelines that we issued under the Gramm-Leach-Bliley Act. Section 501 states that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of customer information. It further directs Federal regulators to establish standards for financial institutions relating to the administrative, technical, and physical safeguards of customer information.

To carry out this broad mandate, the Federal banking agencies issued enforceable guidelines in 2001 that require each bank to have a comprehensive written information security program. Under the guidelines, a bank must first assess the risks both to its customer information and to any methods that the bank uses to access, collect, store, use, transmit, protect, or dispose of its customer information. The bank must then design its information security program to control these risks.

A bank's information security program must not be static. Banks must continuously test their programs and adjust them to address new threats to customer information, changes in technology, and new business arrangements.

OCC examiners review national banks' information security programs. Typically, an examiner will assess the overall adequacy of a bank's security program, as well as specific components of that program. An examiner will consider whether the bank has sufficiently identified the risks to its customer information and then implemented an effective program to manage and control those risks.

But from time to time, things can go wrong, and customer information may be compromised even though a bank has an information security program in place. Where the OCC finds that a bank or its employees or a bank's service provider is at fault, the OCC can bring an enforcement action. The OCC, in fact, has taken a number of enforcement actions to enforce compliance with the secu-

rity guidelines. We have required banks to improve their systems and controls and to notify their customers where warranted.

We believe that a key element of a bank's duty to protect customer information against unauthorized access and use is appropriate notification to customers of security breaches that would compromise their confidential information. Armed with notice, bank customers may take steps to protect their information from misuse, such as by placing fraud alerts on their credit reports.

The information security guidelines, however, do not specifically require banks to notify their customers about security breaches. Therefore, in 2003, the OCC and the other Federal banking agencies took the initiative to propose guidance to address this. I am pleased to inform the Committee that, after considering numerous public comments on this proposal, the agencies have just reached an agreement on this guidance. The OCC signed off on the final guidance earlier this week, and the other agencies are currently in the midst of their individual agency approval processes. Once this guidance becomes final, we expect immediate compliance.

The OCC will consider a bank's failure to follow the final guidance as a violation of the underlying security guidelines. We have a number of remedies at our disposal, including the ability to compel a bank to provide notice to customers about a security breach involving their personal information.

Mr. Chairman, the Gramm-Leach-Bliley Act gave the regulators the direction and important authority to establish information security standards for use by the institutions we regulate. The OCC has found this authority to be well-suited to address the evolving information security challenges that we face. We are committed to using this authority to assure that national banks have adequate procedures in place to safeguard their customers' information.

Thank you, and I am pleased to answer any questions.

Chairman SHELBY. Thank you.

Special Agent Johnson, what trends are you seeing, from your perspective, with respect to the level of the sophistication of the identity thieves? Specifically, do the recent incidents reveal that they are now systematically targeting major data sources—banks and so forth? Can you speak to that?

Mr. JOHNSON. Yes, Mr. Chairman. We are seeing, like my oral testimony, 5 to 6 years ago we saw more low-tech identity theft type of crimes, which evolved into a little more technical with skimming—waiters in restaurants taking your credit card and swiping it through a skimmer which downloads that information and is used. So it is individual. We are now seeing much more intrusions into financial institutions, data brokerages, where thousands and thousands of either credit card access devices are stolen or personal identifiers. And then it is sold on the Internet at some of these websites that pop up daily.

We see other developments into key loggers, keystroke loggers, that are able to record information by keystroke, or even key logger situations on telephones that can download telephone information.

Chairman SHELBY. Sophisticated.

Mr. JOHNSON. Yes, sir.

Chairman SHELBY. How adaptive are these kinds of criminals? Do they probe for vulnerabilities everywhere?

Mr. JOHNSON. Yes, Mr. Chairman. Also, 5 to 10 years ago most hackers saw intruding into a financial institution as a challenge, without criminal intent. Now, with the success of selling this information and gaining monetary means, they have profited, so it has evolved into——

Chairman SHELBY. They see gold there, don't they?

Mr. JOHNSON. Yes, sir.

Chairman SHELBY. Okay. What would be your best guess, if you had a guess, as to who their next target might be, these sophisticated criminals? Anything dealing with electronics, anything——

Mr. JOHNSON. What I can comment on is that the Secret Service, we have analysts, we have agents that, we are looking for that next trend.

Chairman SHELBY. Anticipation.

Mr. JOHNSON. Exactly.

Chairman SHELBY. And you keep that inside of you. Thank you.

Ms. Friend, what can a national bank do to protect itself from large amounts of personally identifiable data that are compromised at another source?

Ms. FRIEND. Are you talking about a situation where a service provider has bank customer information?

Chairman SHELBY. Yes.

Ms. FRIEND. Under our security guidelines, banks are required to oversee the arrangements that they have with service providers. There are several aspects to that. Banks have to use due diligence in selecting a service provider. Banks, by contract, have to require their service providers to have safeguards in place to protect bank customer information. And, if banks determine that their service providers present an undue risk to them, they have to actively monitor those service providers.

Chairman SHELBY. I appreciate both of you appearing here, and we will continue to work this.

I have just been informed that we are going to have a series of seven votes beginning in the next few minutes in the Senate. In light of this, I am going to recess—this will take two or three hours—I am going to recess the hearing and ask that the last panel, who have come from far away, probably, here—and I recognize the inconvenience, but there is not anything we can do about it—that we get with you and reschedule. Not you, Ms. Friend and Mr. Johnson, but the others, the last panel here, ChoicePoint Services, Mr. McGuffy; Evan Hendricks, Editor and Publisher of Privacy Times; and Ms. Barbara Desoer, Executive Vice President, Global Technology, and Service and Fulfillment Executive, Bank of America, that they reappear before the Committee next week. We hate to do this, but we have no choice. This issue is too big and too important not to have you come back.

But Mr. Johnson and Ms. Friend, we thank you for your appearance here.

The hearing is adjorned.

[Whereupon, at 4:24 p.m., the hearing was adjourned.]

[Prepared statements supplied for the record follow:]

PREPARED STATEMENT OF SENATOR JON S. CORZINE

Mr. Chairman, I want to thank you for holding this hearing on identity theft and issues related to the security of sensitive consumer information.

Your response to this emerging problem and the request for a hearing submitted last week by Senators Schumer, Stabenow, Reed, and myself are reflective of the strong leadership both you and Ranking Member Sarbanes have displayed in response to this growing and dangerous weakness in our society.

The importance of this, as we all have heard, has been underscored recently with news of the information breach of a unit of LexisNexis, the scandal at data broker ChoicePoint, and the loss by Bank of America of sensitive information on over one-million individuals, among them Members of the U.S. Senate—including some Members of this panel.

These alarming instances are a stark reminder of just how vulnerable consumers, and each of us, are to having our personal information fall into the wrong hands—hand of thieves. Personal information such as our Social Security numbers, drivers license and auto registration numbers, credit histories, and credit card numbers.

But as equally as alarming as the brashness of identity thieves is the notion that there are likely other instances of large-scale identity theft that have *never* been disclosed to the public.

Mr. Chairman, identity theft is on the rise and is now our Nation's fastest growing consumer crime. According to the Federal Trade Commission, nearly 10 million Americans were the victims of identity theft in 2003, three times the number of victims just 3 years earlier. Research shows that there are little more than 13 identity thefts every minute.

It is a crime that harms our economy in the form of lost productivity and capital. Aggregate estimates of the costs of identity theft are hard to quantify—a problem in itself. According to the Identity Theft Resource Center, identity theft victims spend on average nearly 600 hours recovering from the crime. Additional research indicates the costs of lost wages and income as a result of the crime can soar as high as $16,000 per incident.

Technological innovation has brought about a data revolution that most consumers have benefited from through efficiency, expanding access, product marketing, and lowered costs. And it is spurred the creation on an entire industry of data collectors and brokers who profit from the packaging and commoditization of one's personal and financial information.

But regrettably, this technology has also provided identity thieves with an attractive target, and relative anonymity, with which to ply their sinister trade.

So what can we do to?

Well for starters Mr. Chairman, Congress must recognize the severity of this problem and stop trying to address identity theft in a piecemeal fashion or ignore its reality.

It is ironic that we are holding this hearing today—the same day that the full Senate is likely to pass a Bankruptcy bill intended to protect credit card companies and other financial entities from consumers—but we have yet to act on comprehensive legislation aimed at protecting consumers from having their personal and financial information lost or stolen from those very same credit card companies and financial institutions.

Next week, I plan to introduce the Identity Theft Prevention and Victim Notification and Assistance Act. The bill takes a comprehensive approach to the problem of identity theft—better oversight, strong standards aimed at preventing identity theft, victim notification and assistance, and tough enforcement by Federal regulators.

The legislation improves oversight by establishing the Federal Trade Commission as the primary regulator of nonfinancial third party data collectors. It also authorizes the FTC to write rules requiring firms to ensure the accuracy, security, and integrity of sensitive personal information, and to consider applying the security and personal information safeguard provisions of the Gramm-Leach-Bliley and Fair Credit Reporting Acts to these entities.

The bill would enhance identity theft prevention by requiring *all* companies that maintain sensitive personal information to establish security systems that safeguard that information. The safeguards would have to be in compliance with minimum standards established by Federal regulators, and the company's chief compliance office, or CEO, would have to personally attest to the fact that those safeguards are in place and being monitored on an ongoing basis.

The legislation would also help identity theft victims protect themselves—by requiring companies to immediately notify affected customers, Federal regulators, credit reporting agencies, and law enforcement when the breach or loss of sensitive

customer information has occurred in a manner that could lead to identity theft. This should not be voluntary on the part of the data broker, bank, or credit card company.

Mr. Chairman, this measure is similar to an amendment I offered during the Committee's consideration of the Fair Credit Reporting Act reauthorization bill over a year ago. The provision was dropped due to opposition from the financial services industry and some regulators—including the Office of the Comptroller of the Currency (OCC), which is among the witnesses testifying before us. I hope the reality and severity of the identity theft issue has moved these bodies to a changed view.

Mr. Chairman, notification is vital, because as many as 85 percent of all identity theft victims find out about the crime only when they are denied credit or employment, contacted by the police, or have to deal with collection agencies, credit cards, and bills.

I would point out that the only reason the ChoicePoint scandal became public was the fact that the company was required to notify the public under California law, the only breach notification law of its type in the Nation.

Finally, the legislation includes tough enforcement measures and will allow civil action to be taken by individuals, and State AG's, for violations of this Act that result in identity theft.

I urge my colleagues to support this vitally needed legislation.

In closing Mr. Chairman, I want to again thank you for your leadership on this important issue. I thank you for holding this hearing and I welcome all of our witnesses.

PREPARED STATEMENT OF SENATOR ELIZABETH DOLE

Identity theft is often cited as the fastest growing crime in the Nation. According to Federal Trade Commission estimates, approximately 10 million Americans are victimized by identity thieves every year at a cost of an astonishing $50 billion. And this number is a conservative estimate. Precise statistics are not available to properly gauge the full extent of the problem, since some 40 percent of identity theft cases are believed to involve friends or family members and are never reported.

Today, we will examine two recent incidents in which the sensitive personal information of Americans may have been compromised. The first involves ChoicePoint, a company that provides credit information to businesses. A ring of Nigerian identity thieves posing as a collection agency fraudulently obtained sensitive personal information from ChoicePoint. The second incident involves Bank of America's data tapes that were lost while in transit to a backup storage facility.

We in this Committee and in the Senate as a whole are justifiably concerned about how these situations will be resolved. In the near-term, I applaud Bank of America for their efforts to promptly inform authorities and concerned customers of the missing backup tapes. I am relieved to learn that, according to representatives of the bank, there have been no reports of fraud on any of the accounts in question in the 2 months since the loss of these tapes.

Fighting fraud and protecting the security of personal information is a concern that unites financial institutions and consumers. Each group is harmed by the fraudulent use of personal information. Financial institutions are usually liable for any losses suffered as a result of the fraud, and their customers may be less willing to utilize their services for fear of fraud. Consumers are harmed by the insecurity, inconvenience, and loss resulting from fraud. Consumers also suffer from the fact that at least a portion of financial institutions' fraud losses can be expected to be passed on to consumers in the form of higher prices. There can be no doubt that when fraud is committed, every law-abiding citizen loses.

I am proud of the work that this Committee undertook in 2003 when we designed and approved the so-called "FACT Act," which gave consumers powerful new tools to detect and prevent identity theft. By ensuring access to free yearly credit reports, allowing consumers to place "fraud alerts" on their credit reports, and placing meaningful new obligations on financial institutions to prevent identity theft, this Committee made significant strides toward closing the loopholes that identity thieves exploit. I am confident that we will continue to close these loopholes until identity theft is no longer a growth industry for criminals.

I would like to thank our witnesses for taking the time to join us here today to discuss these issues. And I would like to thank the Chairman for the attention he is giving to resolving issues of such importance to all Americans.

PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

U.S. SENATE

on

IDENTITY THEFT: RECENT DEVELOPMENTS INVOLVING THE SECURITY OF SENSITIVE CONSUMER INFORMATION

March 10, 2005

I. INTRODUCTION

Mr. Chairman and members of the Committee, 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

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

---

at http://www.ftc.gov/os/2003/09/synovatereport.pdf).

[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.

one-time use by a single customer. For example, a data broker may collect information for an employee background check and provide that information to one employer.

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

1. Public Record Information

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

2. Publicly-Available Information

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

---

[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 1.7 million visits to the Web version. The FTC's consumer and business education campaign includes other materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related

---

[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 709,000 hits to the Web version.

B. Working with Law Enforcement

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

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

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

The Commission also encourages even greater use of the Clearinghouse through training seminars offered to law enforcement. Beginning in 2002, the FTC, in cooperation with the

---

[51] Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Feb. 2004) (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 16 seminars across the country. More than 2,200 officers have attended these seminars, representing over 800 different agencies. Future seminars are being planned for additional cities.

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

PREPARED STATEMENT OF LARRY JOHNSON

SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION
U.S. SECRET SERVICE

MARCH 10, 2005

Good afternoon, Chairman Shelby. I would like to thank you, as well as the distinguished Ranking Member, Senator Sarbanes, 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 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 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 websites. 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, finan-

cial institution, medical office, or Government agency. The collusive employee will access the proprietary database, 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 multijurisdictional 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 ECTF's have been added in the last 2 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 cybercrimes 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 2 years, we have held seminars in 18 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 multijurisdictional 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 multicount 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 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 Shelby and Senator Sarbanes, 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.

PREPARED STATEMENT OF AMY S. FRIEND

ASSISTANT CHIEF COUNSEL, OFFICE OF THE COMPTROLLER OF THE CURRENCY

MARCH 10, 2005

Mr. Chairman, Ranking Member Sarbanes, and Members of the Committee, the OCC appreciates the opportunity to testify today about a subject that is critically important to the integrity of the relationship between a bank and its customers—a bank's ability and legal obligation to safeguard customer information. We commend the Banking Committee's leadership in addressing this important subject.

It is a matter of primary importance to the OCC, as it is to the Committee, that national banks have adequate procedures in place to safeguard customer information. My testimony will describe the legal requirements on banks to safeguard customer information, the examination process for assessing the adequacy of a bank's security program, OCC enforcement actions against banks and individuals for breaches of information security, and upcoming interagency guidance that will detail the circumstances under which the Federal banking agencies expect institutions to notify their customers of security breaches.

Background

The OCC routinely examines national banks for the safe handling of customer information. We consider safeguarding customer information to be essential to maintaining the safe and sound operations of a bank. As a result, information security has been a part of our overall supervisory process for many years. The level and extent of our supervisory review has evolved as bank operations and the technology banks employ have become increasingly complex and sophisticated. The OCC has a number of examiners dedicated full-time to conducting information technology and information security examinations, as well as many additional examiners performing these functions for a portion of their time.

Over the years, the OCC, on its own and in conjunction with the other bank regulators, has published guidance and handbooks in this area advising banks of our

expectations about acceptable risk management processes and procedures for safeguarding information, including in the areas of maintaining, transporting, and disposing of information. Further, OCC examination staff and attorneys participate in interagency coordination meetings concerning information security, such as regularly attending and participating in the Attorney General's Council on White Collar Crime, Subcommittee on Identity Theft.

Information Security Guidelines

Section 501(a) of the Gramm-Leach-Bliley Act states that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of customer information. Under Ssection 501(b), the Federal financial institutions regulators are directed to establish standards for financial institutions relating to the administrative, technical, and physical safeguards of that information in order to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

To carry out this broad mandate, in February 2001, the OCC and the other Federal banking agencies issued standards in the form of guidelines, requiring each bank to have a written information security program designed to meet these statutory objectives.

Under these security guidelines, the board of directors must approve a bank's written information security program and oversee its development, implementation, and maintenance. The Board must review annual reports on the status of the program and the bank's compliance with the guidelines.

In developing its information security program, a bank must assess the risks to its customer information and any methods the bank uses to access, collect, store, use, transmit, protect, or dispose of customer information. A bank must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure or misuse of its customer information, assess the likelihood and potential damage of these threats taking into account the sensitivity of customer information, and assess the sufficiency of policies, procedures, and systems the bank maintains to control the risks.

The bank must then design its information security program to control the identified risks. Each bank must consider at least the 8 specific security measures set forth in the guidelines and adopt those that are appropriate for the institution. These measures include access controls on customer information, encryption of electronic information, monitoring systems to detect actual and attempted attacks on customer information, and response programs that specify actions to be taken when a bank suspects or detects unauthorized access to customer information.

Each bank must train staff to implement the program and oversee its arrangements with service providers that have access to bank customer information. This includes using due diligence in selecting service providers, requiring by contract that service providers implement appropriate safeguard measures, and monitoring the activities of service providers where necessary to control the risks the bank has identified that may be posed by the service provider's access to the bank's customer information.

A bank's information security program must not be static. Banks must routinely test their systems and address any weaknesses they discover. Banks must adjust their programs to address new threats to customer information, changes in technology, and new business arrangements.

Examinations for Information Security Programs

The OCC examines national banks for compliance with the security guidelines. In conducting an examination, an examiner will review the bank's written information security program and its implementation in accordance with interagency examination procedures. These procedures include the following determinations:

- whether the program is appropriate for the size and complexity of the bank and the nature and scope of its activities;
- the degree of the board's involvement in overseeing the program;
- the adequacy and effectiveness of the bank's risk assessment, including whether the bank has considered risks to all methods to access, collect, use, transmit, protect, and dispose of information;

- the adequacy of the program to manage and control the identified risks, including technical and procedural controls to guard against attacks, encryption standards used, and monitoring systems;
- whether staff are adequately trained to implement the security program;
- the nature and frequency of tests of the bank's key security controls, the results of these tests, and whether they are conducted or reviewed by independent sources;
- the adequacy of measures to oversee service providers; and
- whether the bank has an effective process to adjust its information security program as needed to address such matters as new threats, the sensitivity of customer information, technology changes, a bank's changing business arrangements, and outsourcing arrangements.

OCC Enforcement Actions and Investigative Activities

From time to time, things can go wrong and customer information may be compromised despite a bank's information security program. The program itself may be inadequate, the systems to protect customer information may be breached, bank employees may not follow the program requirements, or unanticipated risks may arise. An outside service provider that maintains bank customer information on the bank's behalf may face the same issues. Where the OCC finds the bank, the bank's employees, or the bank's service provider to be at fault, the OCC can bring an enforcement action.

Supervisory and Enforcement Actions Against Banks

The OCC has taken various actions to enforce compliance with the security guidelines against banks. In some cases, where the bank had not already done so, the OCC required national banks to notify their customers of security breaches involving their personal information. In another circumstance, the OCC directed a national bank to revamp its employee screening processes.

For example, the OCC issued a cease-and-desist order against a California-based national bank, requiring, among other things, that the bank notify customers of security breaches, after the OCC's investigation revealed that the bank's service provider improperly disposed of hundreds of customer loan files. The OCC also issued a cease-and-desist order against the bank's service provider, and assessed hundreds of thousands of dollars in civil money penalties against the bank and its service provider.

In another case, the OCC, after investigating allegations of a data compromise by a bank employee, directed a retail credit card bank to notify customers whose accounts or information may have been compromised. The OCC was able to determine that the information was used for nefarious purposes, after working collaboratively with the Federal Trade Commission to review complaints of identity theft made to the Commission through its Consumer Sentinel Program, of which the OCC is an information-sharing member.

The OCC also directed a large bank to improve its employee screening policies, procedures, systems, and controls after the OCC determined that the bank's employee screening practices had inadvertently permitted a convicted felon, who engaged in identity theft related crimes, to become employed at the bank. Deficiencies in the bank's screening practices came to light through the OCC's review of the former employee's activities. OCC examination staff and attorneys regularly discuss appropriate employee screening practices and processes with national banks.

Investigations and Enforcement Actions against Bank Insiders

In more than 15 other cases, the OCC has taken enforcement actions against bank insiders who have breached their duty of trust to customers, were engaged in identity theft-related activities, or were otherwise involved in serious breaches or compromises of customer information. These enforcement actions have included, for example, prohibiting individuals from working in the banking industry, personal cease and desist orders restricting the use of customer information, the assessment of significant civil money penalties, and orders requiring restitution.

For example, after the OCC investigated and determined that a Colorado-based bank loan officer and loan processing assistant misappropriated customer information and emailed the information to a third party, the OCC prohibited the two individuals from the banking industry, assessed civil money penalties against each, and issued cease and desist orders against each that placed restrictions on their future use of customer information.

In another matter involving a collections supervisor of a bank, the OCC's investigation revealed that the former bank employee misappropriated customer information, created fictitious Paypal payment accounts, and then embezzled money from the customers' bank accounts, thereafter depositing the money into the fictitious

Paypal accounts. The OCC prohibited the employee from the banking industry, the employee paid tens of thousands in restitution, and the OCC assessed a civil money penalty against the employee.

Many of these data compromise or identity theft cases were initially processed as part of the OCC's Fast Track Enforcement Program, whereby the OCC specifically targets current or former bank insiders for enforcement action based upon criminal authorities' declining to prosecute. Typically, law enforcement relies upon loss amounts in deciding whether to prosecute. However, loss amount from theft of customer information is both difficult to quantify and may not be present for the institution from which the information has been misappropriated. In such cases, the OCC has acted to remove wrongdoers from the industry, and, in appropriate circumstances, ordered restitution and civil money penalties as well. The OCC was also involved with the recent amendment of the Suspicious Activity Report (SAR) form to include a specific check box for identity theft, thereby making it easier for criminal law enforcement and the Federal banking agencies to identify referrals concerning identity theft and data compromise.

Upcoming Guidance on Response Programs and Customer Notice

The OCC believes that notifying customers of a security breach involving their personal information is a key part of a bank's affirmative duty under the security guidelines to protect customer information against unauthorized access or use. While a bank may monitor a customer's account for suspicious activity following an incident of unauthorized access to that customer's information, monitoring will not prevent an identity thief from misusing that customer's personal information at another institution, such as to open a new account at a different bank. Armed with notice, however, bank customers may take steps to protect their information from further misuse, such as by placing fraud alerts on their credit reports that will alert other creditors that these individual may be victims of fraud.

The information security guidelines, however, do not specifically require banks to notify their customers in the event of security breaches involving their personal information; therefore, the OCC is working with the other Federal bank regulators to finalize interpretative guidance stating the agencies' expectation that banks notify their customers of security breaches in appropriate circumstances. I am pleased to inform the Committee that, after considering public comments, the agencies reached an agreement on this guidance last week. The Acting Comptroller of the Currency approved the guidance on behalf of the OCC earlier this week, and the other agencies are now working through their approval processes.

The OCC, along with the other banking regulators took the initiative to propose the guidance in 2003 as an interpretation of the security guidelines. Noting that internal and external threats to a bank's customer information are reasonably foreseeable, the guidance stated that the agencies expect each bank to implement a response program with specific policies and procedures for addressing incidents of unauthorized access to customer information. Specifically, the guidance described the components of a bank's response program. It stated that a bank should assess the nature and scope of the security breach, take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of the customer information, notify law enforcement and the bank's primary regulator of the incident, and notify customers of the incident when warranted, as well as provide customers with helpful information about how to contact the bank with questions and how to place a fraud alert on consumer reports.

The guidance provided that customer notice is warranted when the security breach involves access to information of the type that could easily be misused, such as a customer's Social Security number and account number, which could be used by an identity thief to impersonate an individual and take over the customer's account. The guidance stated that banks are expected to notify their customers of the security breach unless they determine that the breach is unlikely to result in misuse of the customer information.

In crafting the standard for customer notice the agencies have sought to establish the appropriate threshold for when customers may actually benefit from receiving notice. For instance, under the proposed guidance, notice would not be warranted where a bank can immediately contain security breach and establish that the information has not been and is unlikely to be misused. An example of this would be where a bank determines that customer information was destroyed before it could be retrieved or used.

The agencies received a number of comments on the proposed guidance emphasizing that not every breach of information security will result in harm to customers. Commenters stated that providing an overabundance of notices to consumers may have unintended consequences mainly that consumers may initially be

alarmed and perhaps monitor or close their accounts, or place a fraud alert on their credit reports, but eventually may be lulled into complacency by a proliferation of notices. Moreover, commenters maintained that notifying customers of security breaches in every instance could result in the unnecessary placement of fraud alerts on consumer reports and, over time, erode the usefulness of fraud alerts. The agencies agree that some potential for misuse of a customer's information should be present to trigger notice to that customer.

A number of commenters recommended permitting a delay of notice to customers while a law enforcement investigation is pending to avoid compromising the investigation. California law provides for a delay of customer notice if the notice would impede a criminal investigation. The agencies have taken into consideration these and other comments in finalizing the guidance.

Enforcement of Noncompliance with the Guidance

The OCC will consider a bank's failure to follow the final guidance as noncompliance with the underlying security guidelines. The OCC has several enforcement options available to address noncompliance. One option is to use the safety and soundness enforcement process provided by Federal law and OCC regulations. Under this process, the OCC would issue a notice to the bank detailing deficiencies and requiring the bank to submit a corrective action compliance plan within 30 days. An acceptable plan could provide that the bank will adopt measures to correct deficiencies, including notification to customers and restitution for any loss caused by the bank's conduct. If the bank failed to submit an acceptable compliance plan, or failed to materially comply with its compliance plan, the OCC could then issue a Safety and Soundness Order. A Safety and Soundness Order is a formal, public document that is the legal equivalent of a cease-and-desist order. If a bank fails to comply with such an order, the order may be enforced in Federal District Court and the bank could be assessed civil money penalties. The OCC could also choose other enforcement options to address a bank's failure to comply with the guidelines, such as issuing a cease-and-desist order, or assessing civil money penalties.

Conclusion

Mr. Chairman, through the Gramm-Leach-Bliley Act, particularly Section 501(b), Congress gave the regulators the direction and important authority to establish information security standards for use by the financial institutions we regulate. The OCC has found this authority to be well-suited to address the evolving information security challenges we face. We are committed to using this authority to assure that national banks have adequate procedures in place to safeguard their customers' information. Thank you.

IDENTITY THEFT: RECENT DEVELOPMENTS INVOLVING THE SECURITY OF SENSITIVE CONSUMER INFORMATION

TUESDAY, MARCH 15, 2005

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS,
Washington, DC.

The committee met at 10:13 a.m., in room SD–538, Dirksen Senate Office Building, Richard C. Shelby (Chairman of the Committee) presiding.

OPENING STATEMENT OF CHAIRMAN RICHARD C. SHELBY

Chairman SHELBY. The hearing will come to order.

I apologize to you again about disrupting the hearing the other day, but when we had seven scheduled votes, I knew you did not want to come back at 2:00 in the morning. So thank you for coming again today. I recognize that all of you had to shuffle your schedules, reshuffle them a great deal to accommodate the Committee, but this is a very important subject, and I think it deserves our full time and our attention.

Mr. McGuffey, we will start with you. Your written testimony will be made a part of the hearing record in its entirety. You proceed as you wish.

STATEMENT OF DON McGUFFEY
VICE PRESIDENT, CHOICEPOINT SERVICES, INC.

Mr. MCGUFFEY. Thank you, Chairman Shelby, Members of the Committee, good morning. I am Don McGuffey, Vice President of ChoicePoint for data acquisition.

Good morning, I am Don McGuffey, Vice President of ChoicePoint for Data Acquisition and Strategy. I have been with the company since its inception in 1997. The Committee has convened this hearing to address the important issues of identity theft and the security of sensitive consumer information. At ChoicePoint, our mission statement recognizes that in an increasingly risky world, information, through the use of modern technology, can be utilized to create a safer, more secure society. We also recognize the limitations of inappropriate information use as well as the limitations of technology. We know, and have been painfully reminded by recent events, that there can be negative consequences to the improper use of sensitive, personally identifiable data.

As a company committed to the highest standards of information security, we recognize that with respect to the recent events in Los

Angeles, we failed to prevent certain consumer data from being accessed by criminals. For this, we apologize again to those consumers who have been put potentially at risk by this fraudulent activity, and we have and are taking steps to protect them from actual financial harm. We are also working actively with law enforcement to bring to justice those individuals who committed this crime, and we have and will take actions designed to prevent similar violations from occurring in the future.

The modern crime of identity theft, whether in the form of credit card fraud, false business identifications or in other guises, poses a significant threat to all Americans and we support this Committee's efforts to address that danger. In my testimony today, I would like to tell the Committee today about ChoicePoint, describe for you the recent crime perpetrated in Los Angeles, tell you about the steps that we have taken to protect individuals who may have been placed at financial risk as a result of this crime and what we are doing to diminish the likelihood of such incidents from occurring in the future. For example, we recently announced that the company will discontinue the sale of information products that contain sensitive consumer data except where there is a specific consumer-driven transaction or benefit or where the product supports Federal, State, or local government and law enforcement purposes.

Mr. Chairman, ChoicePoint is a leading provider of identification and credential verification services to businesses, government, and nonprofit organizations. We have approximately 5,000 associates in nearly 60 locations. ChoicePoint provides services to 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 companies. Our goal is to put the positive power of information to work for society at-large. We at ChoicePoint are proud of the company's efforts to identify over 11,000 undisclosed felons among those volunteering or seeking to volunteer with community organizations and of our role in helping law enforcement.

Financial and identity fraud is a rapidly growing and costly threat to our Nation's economy. While ChoicePoint offers a large range of tools to help avoid fraud, but no one is immune to it, as other companies and institutions are also learning. This was underscored by recent events in California, which I would like to describe in more detail to the Committee. On September 27, 2004, a ChoicePoint employee became suspicious while credentialling a prospective small business customer based in the Los Angeles area. This employee brought his concerns regarding the application to the ChoicePoint Security Services Department. After a preliminary review, the manager of the Security Services Department alerted the Los Angeles County Sheriff's Department. They decided to initiate an official investigation and asked for our assistance. That investigation is still ongoing, and so far has resulted in the arrest and conviction of at least one individual. As we did in the recent Los Angeles incident, we have worked with law enforcement on other occasions of suspicious activity relating to customer use of our information products. With respect to California, we have learned that those involved had previously opened ChoicePoint accounts by presenting fraudulently obtained California business li-

censes and fraudulent documents. They were then able to access information products primarily containing the following information: Consumer names, current and former addresses, Social Security numbers, driver's license numbers, and certain other public record information such as bankruptcies, liens, and judgments and, in certain cases, credit reports.

Based on information currently available, we estimate that data from approximately 145,000 consumers may have been accessed as a result of unauthorized access to our information products. Nearly one quarter of those consumers are California residents. Since July 2003, California is the only State that statutorily requires affected consumers to be notified of a potential breach of personally identifiable information and authorizes law enforcement officials to delay notification to allow a criminal investigation to proceed. Last fall, we received such a request from the Los Angeles County Sheriff's Department after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time, ChoicePoint had not yet reconstructed all the searches required to identify consumers at risk, and law enforcement officers had not learned all pertinent details of the crime. Working cooperatively with the Sheriff's Department and after completing the necessary reconstruction, we began the process of notifying consumers last month. We elected to utilize the California law as a basis for notifying consumers in all States. Absent specific notification from law enforcement personnel, affected consumers or others, we cannot determine whether a particular consumer has been a victim of actual identity theft. However, law enforcement officials have informed us that they have identified approximately 750 consumers nationwide where some attempt was made to compromise their identity.

Mr. Chairman, our efforts to protect affected individuals did not stop simply with notification in California. We notified consumers nationwide and have taken other steps to assist potentially affected consumers who have identified to date. These include providing dedicated toll-free customer service numbers and a special website to respond to inquiries and to provide information associated with the tools for which ChoicePoint has paid; purchasing and providing free of charge a combined, 3-bureau credit report; purchasing and providing free of charge a 1-year credit monitoring service; and for anyone who has suffered actual identity theft from this fraud, we will provide further assistance to help them resolve any issues from the identity theft.

We hope our efforts will help those individuals take steps to protect their personal data from being used in a criminal manner. In addition, we have taken steps to minimize the likelihood of future occurrences of this nature. We have decided to exit the non-FCRA consumer sensitive data market, meaning we will no longer sell information products containing sensitive consumer data, including Social Security and driver's license numbers, except where there is a specific consumer-driven transaction or benefit or where the product supports Federal, State, or local government and law enforcement purposes. We will continue to provide authentication, fraud prevention, and other tools to large, accredited corporate customers where consumers have existing relationships. We have strengthened our customer credentialling procedures and have em-

barked on a recredentialling process for certain customer segments, including all small business customers. We have created an independent Office of Credentialling Compliance and Privacy that will report to the Board of Directors' Privacy Committee. This office will oversee improvements in customer credentialling processes, the expansion of a site visit based verification program and implementation of procedures designed to expedite the reporting of incidents. This office will be led by Carol DiBattiste, the 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. We have also appointed Robert McConnell, a 28-year veteran of the U.S. Secret Service and former chief of the Federal Government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials.

Chairman Shelby, to conclude, we have all witnessed the significant benefits to society that can come with the proper use of information. ChoicePoint is proud of the role it has played in assisting law enforcement and intelligence agencies as well as vast segments of the American business community in preventing fraud. We have also learned first hand the damage that can be caused when criminals improperly obtain access to consumer information. We have spoken out previously and would welcome a broad national debate on these issues and support efforts by the Congress to provide the independent oversight and increased accountability of entities that handle public record data. We also support increased penalties for theft of personally identifiable information and a reasonable nationwide mandatory requirement for the prevention of unauthorized access to personally identifiable data. As I noted previously, we determined that our commitment to consumers required us to go beyond both the geographic and substantive requirements of existing law and therefore provided nationwide notification and various consumer protection services for those affected. As Congress continues its work in this area, we stand ready as a company to cooperate with your efforts and look forward to participating in the continued discussion of issues related to identity theft and the protection of sensitive consumer information. I would be pleased to answer any questions that you might have.

Chairman SHELBY. Thank you.

Mr. Evan Hendricks, Editor and Publisher, *Privacy Times.* Thank you, sir.

STATEMENT OF EVAN HENDRICKS
EDITOR AND PUBLISHER, PRIVACY TIMES

Mr. HENDRICKS. Thank you, Senator Shelby for the invitation.

A quick housekeeping matter: Since this is the first hearing since Senator Sarbanes announced his retirement, I wanted to thank him on behalf of all constituents for the example he sets of public service, and he will be sorely missed, but think it will inspire many others.

Chairman SHELBY. He is going to be around for 22 more months. [Laughter.]

Mr. HENDRICKS. And I want this subject to be on his to-do list, too, and also, the last time I had the privilege of sitting at this

table, Senator, you told me that we were going to get a good FCRA bill, and we did thanks to your leadership and the work of this Committee and the Congress, and I want to let you know we are already seeing the benefits to consumers in the marketplace.

Chairman SHELBY. Thank you.

Mr. HENDRICKS. That experience and recent events show us that we still have a lot of work to do. The recent events of data leakages at ChoicePoint, Bank of America, LexisNexis, DSW, shows us there are many problems here, and there are many ironies. And one of the ironies is that in order to protect privacy, we need greater sunshine. We need more transparency. There is too much that we do not know.

When a task force was convened in 1973 to decide how do we protect privacy as we enter the computer age, the first principle they established was there should be no information systems whose very existence is secret, and unfortunately, we are bordering on that with the kind of database companies that we have that claim they are out of the reach of the FCRA.

One of the things we need here is a full accounting, an inventory. We need a full accounting first of this episode so we understand what went wrong here. Where are the weaknesses? For instance, Equifax was quoted as saying they sold 8,000 credit reports possibly illegally to ChoicePoint. ChoicePoint sent notices to 145,000 people. Why is this their discrepancy? How did they calculate there were 145,000 people? How long has this been going on? And why did not ChoicePoint or Equifax notice that something suspicious was going on?

I think more broadly, we need an accounting and an inventory of this entire industry. We need to know what Government agencies are providing information to the ChoicePoints and Lexis Nexis, Sizant, Acxiom, and the like. We need to know how do they house their data? How is it organized? We need to know how is warranty card information collected? We know it is collected, but we do not know exactly how. We know when people call an 800-phone number, their information can be captured, a profile can be produced, but we do not know how that information is used and stored.

These are companies that amassed billions of records. The media reports say that ChoicePoint has 19 billion records. That is a lot of records. The problem is that this information, consumers do not have a clear right of access to information that is being held on them. One of my colleagues is Maury Frank. She is an attorney in California who has written about identity theft, and she was at a bar convention meeting, and ChoicePoint had a stand there where they were showing their products, and she said that they put out a 30-page printout from all of their records on her, but they would not give her a copy of the printout. They were just trying to promote their service.

And she noticed there were a lot of mistakes in that, and she said, well, can I get this copy of this? No. How do I correct the mistakes? You cannot. This is basically what I am talking about when I am talking about a secret record system.

Even when consumers do have access for instance, ChoicePoint will say that we have three products: We have a tenant screening product, we have an employment background product, and then, we

have our insurance claims products, and we will give you access to those under the FCRA. In fact, they will give you a free copy. But they say that if they have never sold an employment report, or if they have never sold a tenant screening report on you, then, they do not have a report that you can get access to.

And this raises the fundamental question, if they can sell a report on you, why can they not give access to you? And the thing is what we want consumers to do is to check their reports before transactions so they can ensure the accuracy of the report, but under ChoicePoint's interpretation, they cannot do that, and this is something that we really need to clear up.

I think that most troubling is that it is not clear that they are subject to law and accountable to consumers, they tend not to take responsibility when things go wrong. In my written testimony, I list some examples of run-ins that ChoicePoint has had with accuracy problems or people being disadvantaged by the use of their records. There was one episode where they had purchased information on voters from the Mexican Government and other Latin American countries, but it turned out that itt was done in violation of the laws of those countries, yet, ChoicePoint basically said it was the people who bought the information who were at fault, and they, again, did not take responsibility of it.

In one case, there was a consumer who had problems with their insurance. They had false insurance information simply trying to get the ChoicePoint report cleared up under the FCRA so that they could get insurance at the rate that they were entitled to get it. The thing turned into a Federal lawsuit, and there was a Federal judge in Kentucky named John Heyburn II, who in summing up the case, he wrote that ChoicePoint repeatedly denied making any mistakes and instead seemed to blame all defective data on others. Furthermore, ChoicePoint employees appeared slow to recognize problems, even once they were put on notice and disclaimed all responsibility. Most notably, they seemed annoyed for even having to appear at trial. They never really explained the computer glitches which apparently caused this problem, and to this day, the Court is still unclear what procedures, if any, ChoicePoint uses to ensure the accuracy of its mass circulated reports.

So when there is a full hearing, and someone drills down and looks at the system, we see there are major problems there. And of course, accuracy is one of our first goals of our fair information practices. That is what we want to see in credit reports. These are what we want to see in these other reports. These are reporting agencies. They are just not credit reporting agencies. And the anecdotal report that we have is that there are major accuracy problems—which makes sense. When you have information coming from all sorts of different sources like courthouses and State government agencies and licensing agencies, the more the information moves away from the original source, the more you lose data integrity.

As we look at solutions, I think we need to, again, have a full accounting so that we understand what is going on. I think that we need to look particularly at the use of drivers' data. I think we need to understand in light of all these problems, is it prudent to continue to have, for example, drivers' agencies giving all the driv-

ers' data to companies like ChoicePoint until we know everything that went wrong here, until we know there is full accounting of the system? I think we should consider and the States should consider suspending that information until we have full answers here.

More broadly, we need to extend fair information principles to this database sector to make sure everyone has the right of access to their information, the right of correction, requirements of adequate security, and most importantly the right to enforce their rights when something goes wrong. Whenever you are talking about privacy rights, you are talking about 200 million Americans. You can never build a bureaucracy big enough to enforce those rights, and you do not want to, but you have to empower citizens to enforce their own rights, as we have done in the Fair Credit Reporting Act.

And finally, the California law is responsible for helping us understand that these problems are existing. I know Senator Feinstein is working very hard to make that the law of the land. Many of us favor that, and we just want to make sure that any law passed by Congress is at least as good as the California law.

Mr. Chairman, I want to thank you very much for the opportunity to testify. I look forward to answering your questions.

Chairman SHELBY. Ms. Desoer.

STATEMENT OF BARBARA DESOER
GLOBAL TECHNOLOGY, SERVICE AND
FULFILLMENT EXECUTIVE, BANK OF AMERICA

Ms. DESOER. Mr. Chairman, Senator Sarbanes, Committee Members, good morning. I am Barbara Desoer, Global Technology Service and Fulfillment Executive for Bank of America. I am a member of Chairman and CEO Ken Lewis' executive leadership team, and on behalf of that leadership of our company and all Bank of America associates, thank you for the opportunity to appear before this Committee this morning to provide our perspective on recent events involving our Government charge cardholders.

First, I would like to express how deeply all of us at Bank of America regret this incident. We pursue our professional mission by helping people manage their financial lives. This work rests on a strong foundation of trust. One of our highest priorities, therefore, is building and maintaining a track record of responsible stewardship of customer information that inspires our customers' confidence and provides some peace of mind.

On February 25, 2005, Bank of America began proactively communicating to U.S. GSA SmartPay Charge Card holders that computer data backup tapes were lost during transport to a backup data center. The missing tapes contained customer and account information for approximately 1.2 million Government charge card holders. The actual data on the tapes varied by card holder and may have included name, address, account number, and Social Security number.

Backup tapes such as these are created and stored at remote locations as a routine industry contingency practice in the case of any event that might interrupt our ability to serve our customers. After the tapes were reported missing, Bank of America notified the GSA and also engaged the Secret Service, which began a thor-

ough investigation into the matter, working closely with our corporate information security team.

Federal law enforcement initially directed that to preserve the integrity of the investigation, no communication could take place to the public or to the card holders. While the investigation was moving ahead, we put in place a system to monitor the accounts and, in fact, researched account activity retroactively to the date of the data shipment to identify any unusual or potentially fraudulent activity in the accounts.

The Secret Service has advised us and GSA management that their investigation has revealed no evidence to indicate that the tapes were wrongfully accessed or that their data content was compromised. In mid-February, law enforcement authorities advised us that communication to our customers would no longer adversely impact the investigation. Now, we have completed the initial notifications and are continuing to communicate to our customers to ensure that they understand additional steps we are taking to help protect their personal information.

Bank of America quickly established a toll-free number that Government charge card holders could use to call with questions or to request additional assistance. We also have offered credit reports and enhanced fraud monitoring services to card holders at our expense. Government card holder accounts included on the data tapes have been and will continue to be monitored by Bank of America, and Government card holders will be contacted should any unusual activity be detected. According to standard Bank of America policy, Government card holders will not be held liable for any unauthorized use of their cards.

The incident was unfortunate and regrettable. That said, we feel that it can shed helpful light on the critical element of the industry's practices for data transport. We view this as an opportunity to learn and to lead the industry to better answers that will give our customers the confidence and security they deserve.

As I said earlier, we decided as an abundance of caution to notify the account holders after law enforcement advised us that notification would no longer adversely impact the investigation. However, we also acknowledge that providing notices when there is low risk that the information will be misused has potential drawbacks, such as creating unnecessary anxiety in customers and, if provided too frequently in nonthreatening situations, degrading the effectiveness of a security breach notice.

For example, in some instances, a thorough investigation of the incident may conclude that there was no risk that the information was used for illegal purposes. In these instances, it is probably best to leave it to the discretion of the institution to determine if customers should be notified.

Members of the Committee, I would like to conclude by emphasizing that the privacy of customer information is one of the highest priorities at Bank of America, and we take our responsibility for safeguarding it very seriously. I can assure you on behalf of our leadership team and all our associates, we will do all we can to ensure that our customers have the freedom to engage in business and commerce and to manage their financial lives, secure in the

knowledge that their personal information will be respected and protected by the institutions in which they place their trust.

This concludes my prepared testimony, and I am happy to answer any questions.

Chairman SHELBY. Thank you very much.

Mr. McGuffey, your testimony among other things indicates that ChoicePoint employees first became aware of something unusual on September 27, 2004, and that you began cooperating with California law enforcement officials almost immediately thereafter. As the law enforcement investigation proceeded, you, to use your word, reconstructed the search activities of the suspected criminals and determined the nature and scope of the information that was compromised, and that this took about 3 months.

After this was completed, and after you got the go-ahead from law enforcement officials, you then began to notify affected customers; is that correct?

Mr. MCGUFFEY. Yes, Senator, that is correct.

Chairman SHELBY. Okay; at this point, ChoicePoint also took steps to help those whose information was stolen to protect themselves prospectively. That is, you provided free credit reports, credit report monitoring, and the like; is that correct?

Mr. MCGUFFEY. Yes, Senator, we did.

Chairman SHELBY. Finally, ChoicePoint has decided to get out of the non-FCRA businesses, and that was just a week or so ago. Is that correct, that decision was made then?

Mr. MCGUFFEY. Yes, Senator, I believe it was a couple of weeks ago.

Chairman SHELBY. A couple of weeks ago.

I think it is important for the hearing record for us to correctly establish the sequence of events, and I appreciate you going back through this with me. I know it is tedious.

For further clarification, who, sir, at ChoicePoint was made aware of this situation when it was first discovered in September 2004, in other words, the breach? Was senior management involved in responding to this situation? You are Vice President of ChoicePoint and you have been there from the beginning; is that correct?

Mr. MCGUFFEY. Yes, Senator, I have.

Chairman SHELBY. Let me ask you a question again: When ChoicePoint, found out that you had a breach here in the security in September, who was made aware of that situation?

Mr. MCGUFFEY. The incident was actually discovered by one of the individuals in the credentialling area.

Chairman SHELBY. And who would that be?

Mr. MCGUFFEY. I am not sure of that gentleman's name.

Chairman SHELBY. Would you furnish that for the record?

Mr. MCGUFFEY. Yes, sir.

Chairman SHELBY. Okay.

Mr. MCGUFFEY. After that individual found out, within a day or so, they notified the manager of our security services department.

Chairman SHELBY. Does he report to you?

Mr. MCGUFFEY. No, sir.

Chairman SHELBY. Okay; go ahead. And what is his name? Do you know his name?

Mr. MCGUFFEY. Yes, sir, Robert Kneuth.

Chairman SHELBY. He is a manager of the——

Mr. MCGUFFEY. Security services department.

Chairman SHELBY. Okay; and then, what happened?

Mr. MCGUFFEY. At that point, the security services department and the credentialling group started working cooperatively to try to figure out whether this was, indeed, a real problem, because at this point, what we are aware of is that there is an unusual circumstance in the process of trying to get an account credentialed.

Chairman SHELBY. Let us go over which departments they were again just for the record.

Mr. MCGUFFEY. I believe it is the credentialling department and the security services department.

Chairman SHELBY. The security services became aware of the breach first; is that right?

Mr. MCGUFFEY. Second, actually.

Chairman SHELBY. Second? Who became—the credentials became——

Mr. MCGUFFEY. Yes, the credentials first, because we received a call coming in trying to have a company credentialed to become a customer. At this point, that particular account is not a customer.

Chairman SHELBY. Does this set off an alarm?

Mr. MCGUFFEY. Well what happened was the individual began to be suspicious because of——

Chairman SHELBY. Because it set off an alarm or caution.

Mr. MCGUFFEY. Caution in their head, yes, sir as to how this individual was responding to questions and what kinds of documents——

Chairman SHELBY. Suspicious activity.

Mr. MCGUFFEY. Suspicious activity. They alerted our security department. They then started having a dialogue to try to figure out——

Chairman SHELBY. This was early September?

Mr. MCGUFFEY. Actually, it was around October 1, I believe that the security services department was actually notified.

Chairman SHELBY. When were you notified?

Mr. MCGUFFEY. I was notified on about November 15.

Chairman SHELBY. In other words, there was 6 weeks' lapse between when they were notified of this and when you, as a vice president, was notified of it?

Mr. MCGUFFEY. Yes, sir, actually the notice——

Chairman SHELBY. Can you furnish the exact dates, because I know you have—for the record?

Mr. MCGUFFEY. Yes, sir, I can. I would be more than happy to.

Chairman SHELBY. In other words, who knew what when? What they knew, when they learned it, what they did with it.

Mr. MCGUFFEY. Yes.

Chairman SHELBY. Sequentially.

Mr. MCGUFFEY. Okay; be glad to do that.

Chairman SHELBY. And where did this information go then?

Mr. MCGUFFEY. Prior to November 15——

Chairman SHELBY. Did this languish, now, with two or three people until November 15?

Mr. MCGUFFEY. No, sir, actually, the security services department called in to the home office, which was in Alpharetta. Again, this was happening in Boca Raton, Florida.

Chairman SHELBY. Alpharetta, that is near Atlanta, correct?

Mr. MCGUFFEY. Yes, sir, it is north of Atlanta.

Chairman SHELBY. Who did they call in the home office?

Mr. MCGUFFEY. It came in to our legal department.

Chairman SHELBY. Your general counsel?

Mr. MCGUFFEY. No, not to my knowledge. It went in to one of the staff within the legal department. I will be glad to——

Chairman SHELBY. Furnish this for the record.

Mr. MCGUFFEY. Furnish this for the record, sir.

Chairman SHELBY. What happened to it then?

Mr. MCGUFFEY. They had discussion and then called Los Angeles County to make notice and to try to have a discussion as to——

Chairman SHELBY. But you were aware of what happened at this——

Mr. MCGUFFEY. Not at this time, no, sir.

Chairman SHELBY. What time frame are you talking about now?

Mr. MCGUFFEY. This was in the second week of October, about, and I will be glad to specify and provide to your staff and to this Committee the details exactly, but it was in the second week of October when the dialogue was taking place with our legal department. So at that point, communication went to the Los Angeles County Sheriff's Department.

Chairman SHELBY. And nobody knew that? You did not know that at that time?

Mr. MCGUFFEY. No, sir, I did not.

Chairman SHELBY. Did anybody else know that in your company at your level or higher? Within your counsel's office.

Mr. MCGUFFEY. It was in our legal department, which is part of the—yes, our general counsel's——

Chairman SHELBY. No one was notified by an email or anything? I mean, there are many ways to transmit information.

Mr. MCGUFFEY. Not to my knowledge, sir, but I will be more than happy to provide any other details that I am not currently aware of as part of that investigation.

Chairman SHELBY. Well, what happened then? And where are we now on the calendar?

Mr. MCGUFFEY. Okay; we are in about the middle of October.

Chairman SHELBY. Okay.

Mr. MCGUFFEY. And there is dialogue with the Sheriff's Department, Los Angeles County. They had, at this point in time, not really accepted the case, if you will. We, on the other hand, were still having dialogue with this individual on the other end of the telephone asking for additional documents. In other words, we are trying to keep this individual engaged, if you will, and requesting additional documents from this individual while we are also having conversation with the Sheriff's Department.

Chairman SHELBY. You are part of senior management. You are a vice-president. Was your president, your chairman, any members of the board made aware of this situation?

Mr. MCGUFFEY. Not at this time, no, sir.

Chairman SHELBY. Okay; when were they made aware of this situation? November 1?

Mr. MCGUFFEY. I had a conversation with our president, who I report to——

Chairman SHELBY. What is his name?

Mr. MCGUFFEY. —Doug Carling——

Chairman SHELBY. Okay.

Mr. MCGUFFEY. —in the latter part of November, inquiring as to whether he had been informed of this matter, because it would be not necessarily natural for that notification system to come through me. It would be natural for it to go as it had, which is into the legal department, and be handled as a legal and a law enforcement matter.

Chairman SHELBY. This was the end of November? Before Thanksgiving or after Thanksgiving?

Mr. MCGUFFEY. I do not recall.

Chairman SHELBY. Do you have a log on this?

Mr. MCGUFFEY. No, sir, I do not.

Chairman SHELBY. Will you go back, and there will be something to indicate?

Mr. MCGUFFEY. Attempt to find something; I certainly will.

Chairman SHELBY. Sure.

Mr. MCGUFFEY. I certainly will.

Chairman SHELBY. When was your chairman notified of this?

Mr. MCGUFFEY. To my knowledge, it was in January before a board meeting.

Chairman SHELBY. And he had no inkling of this before then?

Mr. MCGUFFEY. From what I understand and what we have reported, that is correct.

Chairman SHELBY. Who made the decision in the company to provide free credit reports and provide other forms of assistance? Did you do that? Did the president do it?

Mr. MCGUFFEY. I believe that was in conversation between our president and our chairman.

Chairman SHELBY. What was the time frame on this?

Mr. MCGUFFEY. I, again, will be glad to provide the specific data to your staff.

Chairman SHELBY. Was it in October?

Mr. MCGUFFEY. No, sir, it would have been in the middle of February, something in that time frame.

Chairman SHELBY. Who was involved in making the decision to exit the entire line of business that you referenced?

Mr. MCGUFFEY. Again, it would have been——

Chairman SHELBY. Was it the board?

Mr. MCGUFFEY. No, sir, I do not believe so. I believe it was in conversation between our chairman and our president.

Chairman SHELBY. I believe you testified that ChoicePoint, and you correct me if I misstate something, that ChoicePoint took this very seriously when the breach was first discovered; is that correct? Did you consider this a serious situation?

Mr. MCGUFFEY. Yes, Senator.

Chairman SHELBY. A potentially serious situation?

Mr. MCGUFFEY. I believe any time when you have a great deal of dialogue trying to keep someone involved to try to figure out

whether they are fraudulently trying to engage with us and also contacting law enforcement is a serious matter.

Chairman SHELBY. How do you reconcile what you testified to thus far, that in your own words, senior management—of course, you are senior management and others—did not play a critical role in this situation? In other words, were not aware of the situation until later in the game? You say November?

Mr. MCGUFFEY. November is when I was aware, yes.

Chairman SHELBY. Is that right? And yet, in your written statement, you claim that ChoicePoint, "is committed to the highest standards of information security;" in other words, that is central to your business, is it not?

Mr. MCGUFFEY. Yes, Senator, it is.

Chairman SHELBY. If senior management were not aware of what was going on, let alone involved with a major information security breach like this, and you are in the information business, what does that say? Is that the way you all do business in the company?

Mr. MCGUFFEY. Senator, at the time when even I became aware, I was told was that there were only a couple of accounts that were under investigation, so there was no recognition at that time as to the size and the scope of this issue.

Chairman SHELBY. I believe in your written statement, you indicate, and I will quote you, and you correct me if I am wrong on this, "we have worked with enforcement on other occasions of suspicious activity related to customer use of our information products."

The question follows, how many other instances of suspicious activity are we talking about? Are we talking about dozens of times?

Mr. MCGUFFEY. Senator, I am not aware that it is a dozen. I know there are probably a handful of incidents that are related in that manner.

Chairman SHELBY. Would you furnish that information for the record?

Mr. MCGUFFEY. Yes, sir, I shall.

Chairman SHELBY. Have you, sir, in your experience, had other situations like this, did you ever formally consider that clients or potential clients were the most serious information security threat, in other words, the ultimate consumer of this report? That is who the real threat is to, is it not, sir?

Mr. MCGUFFEY. Yes, Senator.

Chairman SHELBY. To their privacy and their information?

In other words, did senior management take steps specific to your business model and the risk associated with it to protect your data and your company? Do you believe they did?

Mr. MCGUFFEY. Yes, Senator, we have spent a great deal of effort on the technology security side to assure that we do not have technology breaches and have technology policies associated with that, have hired outside individuals in order to make sure that individuals cannot hack into our system. And so, we have addressed fairly, I believe, significantly certain risks associated with access. In this case, we had credentialling procedures in place, and unfortunately, we had some fairly sophisticated criminals who were able to circumvent our credentialling procedures and get access.

Chairman SHELBY. Senator Sarbanes.

STATEMENT OF SENATOR PAUL S. SARBANES

Senator SARBANES. Thank you very much, Mr. Chairman. I am sorry I was not able to be here at the outset.

Chairman SHELBY. Go ahead.

Senator SARBANES. First of all, I want to thank you for your leadership on this very important issue raised by the recent breaches of data security and financial privacy. You actually have been a leader in the Senate for many years on the issue of privacy of financial information, and moving on this issue is just another demonstration of that. Millions of Americans are very deeply concerned about this situation.

Chairman SHELBY. Thank you.

Senator SARBANES. *The Baltimore Sun* in an editorial March 2, "Stealing by the Numbers," said that Federal oversight of data brokers is sorely needed, and there should be stiff financial penalties for improper releases. The *Philadelphia Inquirer* on March 6 wrote both episodes, involving ChoicePoint and Bank of America are outrageous instances of businesses falling down on the job after they have been entrusted with vital data. The data leaks demonstrate the need for greater oversight of data bank repositories.

Of course, the data brokers possess many types of information about citizens. *The Washington Post,* in an article, indicated that ChoicePoint has the following types of data on some citizens: and if any of these are not correct, if you do not have these, enter a dissent at the appropriate point: Name, address, and Social Security numbers, automobile and insurance claims history, credit history, vehicle ownership, public records which would contain liens and judgments, military service, educational history, names and addresses of neighbors and relatives, birth, marriage, and death certificates, fingerprints and DNA.

They do not assert that you have it on all citizens but that you keep this kind of very extensive data on at least some citizens. Is that accurate?

Mr. MCGUFFEY. Senator, you read through the list fairly quickly, and I think the one or two that I would——

Senator BUNNING. Read it slowly.

Mr. MCGUFFEY. —make comment on would be on the educational history. The educational history that we may have would be only on those individuals whom we would have performed a preemployment background screening check and only in those instances where our customer would request us to have validated information on an application for a job.

On the military records, we really do not have what I would call military records. We do have historical data prior to 2001 on individuals that may be in the military.

Senator SARBANES. Well, I take it in effect that is a confirmation of the article, though, because in effect, the article does not assert that you have all of this information on everybody, but it does assert that you have it at least on some citizens, so, I mean, it gives some sense of the parameters of the kind of data you collect and how extensive it is in its coverage. I mean, is that a fair statement?

Mr. MCGUFFEY. I would agree, Senator, it is a reasonable statement.

Senator SARBANES. Mr. Chairman, in the face of corporate data banks holding and selling such an extensive array of data on citizens, this issue of data privacy, security, and identity theft obviously takes on particular importance, and I think your analysis in this hearing has focused on it, and I commend you for that.

Chairman SHELBY. Thank you.

Senator SARBANES. It includes consideration of the situation of the consumer both before and after a data security breach. Should a consumer have rights to notice, access, and correction of data held in a data repository? Should a consumer be able to prevent his or her personal, nonpublic data from being included in certain data banks for resale? I mean, you, in effect, sell the data, correct? I mean, that is your business. That is where your income comes from, correct?

Mr. MCGUFFEY. Generally speaking, yes, I would agree with that.

Senator SARBANES. Should Federal minimum data security standards be required for data brokers? What should a data repository be required to do after a breach occurs to prevent consumer fraud and identity theft? And of course, we face the basic question, which we have had to discuss in here before, of whose property is a person's financial information, a consumer's or an institution's?

Mr. Chairman, I remember when we did a hearing, Phyllis Schlafly came before the Committee.

Chairman SHELBY. We did. Had Ralph Nader and Phyllis Schlafly together on the same issue right here.

Senator SARBANES. Exactly. And, of course, she took the very strong position this is a property right, and it belongs to the institution. And in effect, their property rights are being—it was a very interesting——

Chairman SHELBY. There was pretty good agreement between both the left and the right.

Senator SARBANES. It was an interesting concept, and I still recall it.

I received a letter from a constituent saying that he had received a letter from ChoicePoint informing him that a fraud may have resulted in personally identifiable information such as your name, address, Social Security number, or credit report being viewed by businesses that should not have access to such information. So he received a letter from you telling him that.

One of the things he says in his letter to me, he says obviously, this letter from ChoicePoint is very unsettling. The use of the word "may" indicates that ChoicePoint does not know what information was released and demonstrates their inadequate security procedures.

What do I say to him? Of course, one of the things that I will say to him is that you were here, and I had the opportunity to ask you this directly, but what is your response? Of course, his focus now is not that the information went out but that ChoicePoint does not really know by saying to him may what information went out; is that correct?

Mr. MCGUFFEY. Senator, we regret and are deeply sorry that we had this event and the criminal activity associated with it. We did have to take, and a lot of times, as I believe the Chairman had indicated earlier, to recreate all of the various different individual searches that had been instituted against our databases, and in those cases, we actually went back for each and every one of those searches and recreated it.

The information—and my expectation is that the information does actually exist, although in sending out the letters that we sent, we generally patterned that notice after the California law in making notice to those individuals, but my expectation is in that particular case, the details are there.

Senator SARBANES. I have run over my time, so let me just close. This constituent went on to say he recommended these actions, and if I could get a quick reaction, I apologize to my colleague: A data broker company must obtain written approval from the person before any personal information can be given out. That is one recommendation. The other is the data broker companies must be held liable for a person's identity theft and bear the full and total cost to reestablish the person's credit rating and identity. They should also incur punitive damages for their security malpractice.

Can each of you give me a quick reaction to that? Mr. Chairman, I appreciate your indulgence.

Chairman SHELBY. That is okay.

Mr. MCGUFFEY. Senator, one of the concerns that I would have of requiring any individual to consent to the release of the information is related to the activities associated with investigations. I had made the comment earlier in my statement about the variety of services that we have and, indeed, the 11,000 criminals that we had identified that through the process of performing screens, identified the fact that these individuals may have been harmful.

The investigative process, it seems to me that if we have a criminal or someone who was trying to do harm, it is not likely that they are going to give their consent to allow law enforcement or others to investigate that individual.

Senator SARBANES. Well, let us have a law enforcement exception. Does that take care of it?

Mr. MCGUFFEY. What we have taken as a position along those lines is that we should use the principles that are contained in the Gramm-Leach-Bliley Act that was passed, I believe, back in 2001 and some of the principles that are contained in the Fair Credit Reporting Act and apply those to public record data.

Senator SARBANES. And what about bearing the full and total cost to reestablish a person's credit rating and identity when there has been identity theft?

Mr. MCGUFFEY. I suppose, Senator, that we were also the victim of a crime, and it does not seem at least to me at first blush that in that case, where we believe we had reasonable procedures in place to try to prevent a crime, that that would be entirely appropriate, but we obviously would like to engage in that debate with you and the Committee.

Senator SARBANES. All right; Mr. Hendricks, real quick.

Mr. HENDRICKS. Thank you. Quickly, I agree with my fellow Marylander that that is exactly what we need. You cannot have

large organizations enjoying the benefits of trafficking in our personal data if they are not going to take responsibility for it, and I am very troubled by the questioning where you hear about a breach in September, and then, ultimately, it trickles up to senior management by the turn of the year. That is very troubling.

I have had the opportunity to talk to one person who received the ChoicePoint letter, and working with that person, we found out that a couple of years ago, he was called by his Discover Card, and he was asked have you changed your address? Because somebody—this is what the thieves did in this case. They were trying to change the address. And it looked like Discover helped catch that, but these two New Jersey addresses turned up on his credit report and the credit report is the epicenter of this crime.

So he gave me these addresses, and I tracked both addresses down to Mail Boxes, ETC., indicating that these were the drop slots of identity thieves. So there is a lot to be found out here if we have a real joint effort to work here with the consumer. There is valuable data on those consumers' credit reports, and it is a bit disturbing to me that a lot of time has gone by, and valuable leads might have been lost.

Senator SARBANES. Did you want to add anything, Ms. Desoer?

Ms. DESOER. From the perspective of Bank of America, we do not sell our information to any third parties, and we give customers the option to opt out of any sharing of information within our own company that could be used for cross-marketing purposes.

We do have a policy that does not hold the consumer liable for any losses on the product because of fraud, and then, we work with customers on an individual basis to determine what the circumstances are and what else we might be able to do to help them.

Senator SARBANES. Thank you very much.

Thank you, Mr. Chairman.

Chairman SHELBY. Senator Bunning.

STATEMENT OF SENATOR JIM BUNNING

Senator BUNNING. Thank you, Mr. Chairman.

Ms. Desoer, 1.2 million customers lost records, 900,000 in the military; is that correct?

Ms. DESOER. That is correct.

Senator BUNNING. That seems beyond comprehension to me that that happened with one of the biggest banks in the country, 5, maybe 10, but 1.2 million? You are going to have to give me a better explanation than you gave the Chairman.

Ms. DESOER. Okay; what we have as a process in the agreement that we have with our client, the GSA, is that for contingency and data recovery purposes, every day, we back up the data on the entire GSA charge card SmartPay portfolio, and we ship that data to a recovery backup site across the country.

Senator BUNNING. Electronically.

Ms. DESOER. No, these are tapes——

Senator BUNNING. These are backup tapes.

Ms. DESOER. Backup tapes that are taken a slice at a point in time of all of the transaction records for those cardholders and are physically moved. Those tapes are physically moved across the country was the process that happened.

Senator BUNNING. Okay. You explained that nothing has happened, and there is no use, or you have not found any?

Ms. DESOER. Correct.

Senator BUNNING. What is to prevent somebody from holding that data for a year or a year and a half and then using it?

Ms. DESOER. A couple of things: First of all, the data is not easily recoverable. The tapes that were lost were part of a larger set of tapes that in concert need to be run together on specialized equipment using specialized software that require particular expertise and knowledge about how the data is fragmented on those tapes to reconstruct it; not to say it is impossible, but it would—an average person cannot reconstruct that, so in theory, they could.

Senator BUNNING. How much money does Bank of America spend on securing data, that type of personal data?

Ms. DESOER. I would need to get back to you on that particular. I can get that information.

Senator BUNNING. I would like to know exactly how much money they spend.

ChoicePoint Services, Inc., how much money does ChoicePoint spend on securing data, making sure that consumers' information is kept secure?

Mr. MCGUFFEY. Senator, I do not have that figure with me, and I would be happy to——

Senator BUNNING. Would it not be nice to, since you are make money selling information that obviously should not have been sold, it would be nice to know how much money you are spending to secure the data you should not be selling in the first place.

I want to go back to the case in Kentucky, because I personally know the judge. In the case of *Mary L. Boris* v. *ChoicePoint Services,* and Western District of Kentucky, March 14, 2003, Judge John Heyburn on appeal found that one could infer from the evidence that ChoicePoint included incorrect data on plaintiff's claim report; that plaintiff complained about this false information; and that after the original mistakes were corrected, more incorrect claim data reappeared on her report and remained well after the suit was filed.

Based on this series of events, a jury could certainly conclude that a reasonable, prudent company would have prevented a similar outcome. He added, this is Judge Heyburn, "to this day, this Court is still unclear what procedures, if any, ChoicePoint uses to ensure the accuracy of its mass circulated reports."

That is a Federal District Judge, the Chief Judge of the Western District of Kentucky. Now, what did you have to say about that? What did your lawyers have to say about it?

Mr. MCGUFFEY. Senator, I have not personally had conversation with our lawyers about this particular case. We handle 100 million transactions probably a year, and unfortunately, this one appears to be one where we had inconsistencies in our data associated with the record.

Senator BUNNING. Okay; answer this question, then: What procedures does ChoicePoint have in place so that a consumer can make corrections of inaccurate information they find in your database and make it stick and not reappear on your database?

Mr. MCGUFFEY. Senator, in this case, this was an insurance-related incident, and it is covered by the Fair Credit Reporting Act. So we comply with the Fair Credit Reporting Act, where in case of a consumer who is interested in understanding, can get a report, does get a report, and if there is a dispute, we have dispute processes in place, and if you like, I would be more than happy to provide a detail of those dispute processes for you and your staff.

Senator BUNNING. I would like that.

There are many more questions, but I see my time has expired. Thank you, Mr. Chairman.

Chairman SHELBY. Thank you.

STATEMENT OF SENATOR CHARLES E. SCHUMER

Senator SCHUMER. Thank you, Mr. Chairman. I want to say I share my colleague from Kentucky's outrage about this, and, you know, what happened here just boggles the mind, that you actually sold information to criminals who used it for criminal purposes. I mean, if banks operated like ChoicePoint, bank robbers would not need guns. They would open an account, walk in, and take all the money they wanted out of the safe.

It is just amazing, because, and we all know what happens, as Jim has talked about, when somebody has their identity stolen. It takes them on average 175 hours to get it back. So you did not just sell their identities to these crooks; you sold their peace of mind. And the attitude of this company is just casual. I mean, the questions you do not know after these mishaps? You do not know much money is being spent to protect people's identities? You are a vice president of the company?

The time lapse that Senators Shelby and Sarbanes elapsed, how is it that the CEO did not know that thousands of people's identities were stolen until a couple of months later? You tell me: Why did you not call law enforcement immediately? Do you know how much damage might have been done between the day you found out or your company found out and the day you notified law enforcement?

Do you have a policy when somebody's identity is stolen—that is a question—about notifying law enforcement immediately? Does the company have a policy to do that? Yes or no?

Mr. MCGUFFEY. I am not aware as to whether we do or not, but I will certainly provide that——

Senator SCHUMER. Well, why are you here, sir, if you are not aware of a question like that after everything that has happened?

Mr. MCGUFFEY. I was invited by the Committee, sir.

Senator SCHUMER. All right; well, the company chose you to come, right?

Mr. MCGUFFEY. I believe that is correct.

Senator SCHUMER. Did you get briefed?

Mr. MCGUFFEY. Yes, Senator, I did.

Senator SCHUMER. And that question never came up?

Mr. MCGUFFEY. No, Senator, it did not.

Senator SCHUMER. And neither the question about how much money you spend to protect people's identities?

Mr. MCGUFFEY. No, Senator, it did not.

Senator SCHUMER. Let me ask you another one: Have there been other instances where ChoicePoint has been aware that people's identities have been stolen but that has not been made public?

Mr. MCGUFFEY. In these instances, there have been two or three, as I had indicated earlier, and all of those—

Senator SCHUMER. Two or three instances?

Mr. MCGUFFEY. And in all of those cases, we have made notice and in that 145,000——

Senator SCHUMER. Immediately?

Mr. MCGUFFEY. As soon as we were able to recreate the searches, Senator.

Senator SCHUMER. But I am asking, there were rumors that a couple of years ago, this happened, too, and that has not been made public. Is that true?

Mr. MCGUFFEY. No, Senator. In those cases, we found out about the 2002 incident, which may be what you are referring to.

Senator SCHUMER. When did you find out?

Mr. MCGUFFEY. In those cases, we found out in the fall of 2004, because we did an internal investigation and found cases that——

Senator SCHUMER. How is it that identities that you have are stolen or information is stolen, and you do not know until 2 years later? You got no complaints?

Mr. MCGUFFEY. To my knowledge.

Senator SCHUMER. Did you check to see if you had complaints?

Mr. MCGUFFEY. To my knowledge, no, sir.

Senator SCHUMER. And did the company check to see if they had complaints?

Mr. MCGUFFEY. Yes, Senator, those complaints do come in to a central environment.

Senator SCHUMER. Okay; so, were there complaints between 2002 and 2004 that came in to the company?

Mr. MCGUFFEY. With regard to this incident, not that I am aware of, sir.

Senator SCHUMER. And does that mean no, or does that mean you may just not be aware? I mean, did you check? Did you ask before you came here today?

Mr. MCGUFFEY. Yes, Senator, I did.

Senator SCHUMER. And they said?

Mr. MCGUFFEY. No.

Senator SCHUMER. Okay; you do not have to say, then, not that you are aware of; no, you checked.

Have you notified customers before this last situation? In those situations, did you notify customers about the thefts when you found out about them?

Mr. MCGUFFEY. Senator, in these cases, when we did our internal investigation was when we found the various accounts that had been misrepresented to us, and in all of those cases, we made notice.

Senator SCHUMER. To every customer, not just in the States that had a law that you had to.

Mr. MCGUFFEY. Absolutely.

Senator SCHUMER. Okay; let me ask you about your executives. I think this stinks from the head. What about these executives taking $16 million in the months after the company learned that the

database had been breached? Now, I understand the executives are arguing based on their recent 10(b)(5)(1) trading plan, they have a contract to sell these stocks weekly, but according to my understanding and the SEC's rules, those plans can only be entered into if they are entered into in good faith and not as part of a plan to scheme or evade the insider trading rules.

So my question is did the ChoicePoint board of executives and executive officers in question work together to approve a new stock trading plan on October 26, 1 day before the LAPD was tipped off by the company?

Mr. MCGUFFEY. No, Senator, I do not believe that they did. In fact, what I believe that the position of the company and the communication that we provided, although this incident is currently under investigation by the SEC, is that the individuals in question did not know about this until after those plans had been put into place.

Senator SCHUMER. Do you think they should return the money on their own? I think that is what most people would think.

Mr. MCGUFFEY. I am not sure that my opinion, sir, is relevant here.

Senator SCHUMER. Oh, it is relevant.

Mr. MCGUFFEY. Well, in my view, they followed the regulations. The 10(b)(5) plans were put in place by the SEC.

Senator SCHUMER. Let me tell you: I think they should return the money on their own. I will tell you something else I think: I do not know what the law is here, but just from an ethical point of view, you are dealing in important valuables about people. Your attitude has been casual, to say the least; that is putting it kindly. I do not think ChoicePoint should be in business to do anything to do with people's private information. I know you are not selling Social Security numbers to some people, but you are still selling them to State and local governments: Is that right?

Mr. MCGUFFEY. Yes, sir.

Senator SCHUMER. And law enforcement.

Mr. MCGUFFEY. And law enforcement under permissible purpose, yes, sir.

Senator SCHUMER. Well, I would urge any credit company that has this information not to give it to ChoicePoint, because their attitude is just casual, not caring, the kinds of questions that after a major egregious mistake was made should be on the tip of the witness' tongue who was chosen by the company to come are not.

I mean, I think we can do a lot better, and a lot of other companies can do better. Now, I have a question for Ms. Desoer.

Ms. DESOER. Yes.

Senator SCHUMER. My view here is different. I think BofA, Bank of America, was very careful, and when this happened, they notified people immediately. Obviously, this problem occurred. So, I have two questions for you as a result of what happened, how we can make this better.

One, should we do much better screening of cargo handlers, particularly cargo handlers who handle this kind of vital information? And two, would it not be a good way to avoid these incidents by using the RFID technology, radio frequency identification to track

cargo? It is very cheap, as I understand it. It would let us know where everything was.

You know, these thieves stole the wrong thing, but we still know where they are and who had it, et cetera. Does your company have a position on either of those two things as a result of what has happened here?

Ms. DESOER. Yes, Senator, in terms of the tracking, there is tracking that lets us know where the package is at all times with all the carriers that we use.

Senator SCHUMER. Is that an RFID?

Ms. DESOER. I do not know if it is an RFID.

Senator SCHUMER. I suggest you find out.

Ms. DESOER. I will.

Senator SCHUMER. Because if it is stolen, the tracking system that you might have that A passed it to B who passed it to C, and they call you up, is gone, while an RFID would know exactly where it is.

Ms. DESOER. At what stage; that is correct.

Senator SCHUMER. Do you not think that, off the top of your head, would make some sense?

Ms. DESOER. That makes sense.

Senator SCHUMER. Yes.

Ms. DESOER. And in this particular case, we are no longer sending these tapes via courier, so they are going by ground transportation to a different location.

Senator SCHUMER. Right.

Ms. DESOER. And in response to your first question, we think this is an opportunity to revisit the whole issue of how we do send information and send tapes, and we are in the process of doing that.

Senator SCHUMER. Okay.

Thank you, Mr. Chairman.

STATEMENT OF SENATOR WAYNE ALLARD

Senator ALLARD. [Presiding.] Thank you, and I am sitting in here temporarily for the Chairman.

Senator SCHUMER. You are doing an excellent job, I might say, Mr. Chairman, Mr. Temporary Chairman.

Senator ALLARD. It is getting to be funny at the time.

Senator SCHUMER. That is why I said it.

Senator ALLARD. First of all, I ask unanimous consent that my full statement be made part of the record, and without objection, we will so do that

Senator ALLARD. And then, I have a couple of questions.

This Committee has in the last 2 or 3 years gotten involved with the credit score, and I think that many on the Committee did not realize how deeply embedded the credit score was and the credit rating and how just some small change can have a fairly profound impact on your credit rating; for example, the number of charges that were put on your credit card, the number of times you applied for a credit card would all have an impact on your credit score.

And when you go to losing your identity, and it gets manipulated out here in the underworld, I can see really an impact on credit score. What can you do as companies to correct what is happening

to the credit score? Maybe Mr. McGuffey, you would like to, and then Ms. Desoer.

Ms. DESOER. Desoer.

Senator ALLARD. Desoer. Maybe you would both like to respond.

Mr. MCGUFFEY. Senator, we are not a credit company, first of all, as you may be aware.

Senator ALLARD. I know that, but it does have an impact on the credit score.

Mr. MCGUFFEY. It may; it may indeed have an impact, and the only real answer may be for us to evaluate in our actuarial models that build those scores and determine whether there are facets of or features of or line items within the credit report that may be more impacted than not in a situation of identity theft; for instance, I do know that if someone were to put a security alert on their credit report that we pass that security alert along with the score to our end user customer, so our end user customer would be aware that the individual has placed a security alert on their score, on their credit report, and therefore be in a position to take some action on that or be conscious of that, inquire of the consumer as to whether there were anything on the credit report that may have adversely impacted that score.

Senator ALLARD. Ms. Desoer.

Ms. DESOER. From our perspective, we are very much in the business of providing credit, and along with that comes advice about ways that consumers can enable themselves to get credit, so that is part of our business. We increasingly supplement the scores with other kinds of information, because a big part of our population, for example, are people who are new to the country who might not have an established credit score, and so, we use alternatives like records of paying rent and that thing to supplement credit making decisions in addition.

But again, we work very closely with our consumers and on an individual basis, we will help give them advice as appropriate.

Mr. HENDRICKS. Senator.

Senator ALLARD. Yes, go ahead, Mr. Hendricks.

Mr. HENDRICKS. Because you ask—and it is a very important question, because the main damage from identity theft is then, you get all these fraudulent, unpaid accounts, and it causes your credit score to take a nosedive. Companies can help because the credit score is based on your credit report, and the credit reporting agencies believe what the credit granters tell them.

So if a Bank of America or a ChoicePoint is involved, and if they know the information is wrong, if they will help the consumer communicate that to the credit reporting agency, it helps get the bad news off a lot quicker.

Senator ALLARD. Okay; and if you put a security alert on an account, does that suggest that they do—Mr. McGuffey brought that up. Does that help you in getting your loan, or does that hinder you?

Mr. HENDRICKS. Well, in a security alert, it is supposed to make them careful about disclosing that report. Now, in the past, it was not working that well, and this Committee helped pass a law which is supposed to bring better respect for those security alerts.

Senator ALLARD. But if I go in, and I am buying a house, and all of a sudden, I have a security alert on my score, I can imagine that it may very well slow down my loan, and I guess it could cause some problems. But I guess it is a tradeoff, is it not?

Ms. DESOER. That is correct.

Senator ALLARD. Between how far you want to protect somebody, but yet, if somebody needs that credit score, it cannot slow them down.

Mr. HENDRICKS. And in California, they can put a freeze on their credit report, and the victims of identity theft do that, but if they want to get credit, that means they have to unfreeze the report. So, yes, it is not a fun situation either way.

Senator ALLARD. No, it is a problem.

Okay; Ms. Desoer, how long did Bank of America have to wait before informing its customers about the loss of personal information on 1.2 million Government charge cards?

Ms. DESOER. The tapes were lost late in December, and we notified customers or began notifying customers on February 25. We became aware of the loss of the tapes right after the New Year, and very shortly thereafter, once we reconstructed the information and knew that customers' information was on the lost tapes, we got the Secret Service involved, who asked us not to share knowledge of this with the public or with our cardholders until they could get further into the investigation, and as soon as they released that hold on the information, we went ahead and notified customers.

Senator ALLARD. And so, how long did it take you to reconstruct that information, and how long did the investigators ask you to hold that information before you notified the consumers?

Ms. DESOER. It took us about a week to reconstruct that information, and I can get exact dates if you like, Senator, and then, the Secret Service was engaged on January 10, and they released the hold on the information just before we went public February 25, so a day or two before.

Senator ALLARD. So it took them quite awhile to do that investigation.

Ms. DESOER. Yes.

Senator ALLARD. It seems like, and I assume that was a pretty high priority as far as you know.

Ms. DESOER. Yes, it was very high priority for us and our corporate information security team, who was working jointly with the Secret Service in tracking the tapes every step of the way and reconstructing where they were and who was dealing with those, and it still is an ongoing investigation.

Senator ALLARD. What was the first item of information that the Bank of America provided customers informing them of that incident? That was February, then?

Ms. DESOER. February 25, correct.

Senator ALLARD. February 25. And do you feel that this information was helpful to the individual customers? In other words, what steps could customers have taken to actually protect their identity from theft?

Ms. DESOER. It is a great question, sir, and what we did, it is always a balance of what it is we are trying to communicate, because these customers, the information was presumed lost, and

there had been no evidence for these customers that there was any misuse of their information.

So it was an awareness of what had happened, an indication of an 800-number where we would be in a position, for example, to share with them individually, exactly what information was on the tapes as it related to them as an individual, and then, we also used it as an opportunity to communicate a list of activities that the consumer could take to protect themselves on an ongoing basis against identity theft.

In addition, we made available free of charge to the consumer a credit report if they wanted additional verification that there had been no activity and fraud monitoring services. And of course, we were monitoring their accounts retroactive to day one when the tapes were lost, and we continue to do that.

Senator ALLARD. What did you lose from the loss, from this incident where you lost information? What did you learn?

Ms. DESOER. Oh, what did we learn?

Senator ALLARD. Yes, what did you learn when this information—when you had this incident where you lost information?

Ms. DESOER. That we need to revisit the standard industry practice of shipping tapes in this way for contingency and backup data recovery purposes.

Senator ALLARD. So you learned that you need to do more on data backup recovery; that you need to do something different as far as how you are transporting this information.

Ms. DESOER. No, we need to stay committed to the path that we are on of data backup recovery, that it is very important that we comply with each of our contracts and with requirements under which we operate that, for certain types of data, set the time lines in which after, say, a hurricane or an event that would take out a data center, we need, within hours in some cases, 2, 4, 24, 48 hours, to be able to be up and running again on behalf of our customers.

That is in place, and that remains in place. What we are in the process of reconsidering is the way we get the information from point A to point B.

Senator ALLARD. I see. Anything else you learned? Have you taken corrective action once you have learned these things?

Ms. DESOER. Yes, we have stopped shipping the tapes the way we have; we are working closely with the customers with whom we have communicated, and it is a reinforcement, and we followed very standard policies and procedures that we have in place at Bank of America for dealing with events such as this, and it reinforced for us that it is a good process and works well.

Senator ALLARD. Thank you.

Ms. DESOER. Thank you.

Chairman SHELBY. [Presiding.] Thank you, Senator Allard.

Mr. McGuffey, how large is your counsel office? In other words, how many attorneys work in your counsel's office?

Mr. MCGUFFEY. I believe, Senator, that there are four lawyers today.

Chairman SHELBY. Four lawyers? And how many support people roughly?

Mr. MCGUFFEY. I do not know exactly, but I would say that there is probably a dozen would be my guess.

Chairman SHELBY. Is a lot of the focus in that counsel's office to protect or to focus on possible breaches of information in all of this and the legal ramifications that perhaps go with it?

Mr. MCGUFFEY. There is a set of staff that are focused on reviewing incidents and audits. There is an audit program that we have in place that goes back and audits customers, and indeed, in this case, the reference to the 2002 incident that was made earlier, that particular account was shut down, I believe, in May 2002 as the result of an audit. So we audit our customers, and that is part of that team. We review subpoenas in that team as well as responding to litigation and other matters, other legal matters.

Chairman SHELBY. Would you for the record furnish a summary of the sequence of events dealing with when counsel was involved, exactly when they notified who in the company, your company, or outside, who they dealt with and so forth? Could you do that?

Mr. MCGUFFEY. Yes, Senator; yes, Senator, we will.

Chairman SHELBY. If the facts in this case from what you have said did not lead to an immediate notification of senior management—and this has been your testimony—can you help me understand a situation where your senior management would be notified immediately? In other words, what would it take to notify them, your president, your chairman, perhaps some of your board members that this is a serious situation, which it was? What would it take? What kind of situation would it take?

Mr. MCGUFFEY. Senator, I am——

Chairman SHELBY. Just help us understand.

Mr. MCGUFFEY. I am certain that there are a number of matters, as there are a variety of disciplines, there are a variety of departments, obviously, that report to both those individuals, and any of the major events associated with those disciplines as perceived by those individuals at the time would probably be appropriate and probably are discussed with those superiors, and what I would like to make sure the Committee understands is that at the time in the fall of 2004, we were aware of only a handful of accounts that we believed were problematic.

The investigation continued, and we continued to try to find and identify accounts that were similar in nature. We did our investigation to find additional accounts, even beyond those that were identified by our employee in the credentialling process.

In the future, our CEO has required that he will be notified of any of the breaches that could lead to any serious intrusion into our systems, any law enforcement activity associated with this type of activity, so we are setting up processes; in fact, I had indicated earlier that we have even set up a new department that will be reviewing these matters headed up by Carol DiBattiste, and we are looking forward to her joining our management team, and I am certain that she will also make additional changes and recommendations associated with how we proceed with these matters.

Chairman SHELBY. You can tell there is concern here with the fact that there was a gap between—from your testimony—between discovery of the breach and the notification of people up the line. If a lot of people were in senior management of your firm, I think

there would be concerns about the fact that they had not been notified, and that would be cause for probably some discipline there, who knows, and change of policy. Have there been any dismissals of personnel because of failure to notify up the line for something this serious? It is so central to your company and the well-being of your company and perhaps the future of your company.

Mr. MCGUFFEY. Yes, Senator, it is a very serious matter, and we regret in this case——

Chairman SHELBY. But there have been no personnel disciplined, dismissals of people because of their conduct regarding this?

Mr. MCGUFFEY. In this case, Senator, no, the activities were handled as a law enforcement and a legal matter, and those personnel were informed.

Chairman SHELBY. How does your firm make sure, Mr. McGuffey, that you are complying with each of the applicable laws such as FCRA and GLBA that govern the use of information in your possession?

Mr. MCGUFFEY. We have both legal counsel who advises the businesses with regard to those matters. We have technology infrastructure.

Chairman SHELBY. Do you do an audit?

Mr. MCGUFFEY. Yes, we do. We have both an internal audit department as well as an audit group within our legal department that focuses on these types of matters.

Chairman SHELBY. How frequently do you do your audits, check on your customers?

Mr. MCGUFFEY. It is a continuous process.

Chairman SHELBY. Okay; have you ever terminated customers based on violations of the fair credit laws and the Gramm-Leach-Bliley Act?

Mr. MCGUFFEY. We have, indeed, yes, Senator, and also terminated accounts that did not pass through our audits.

Chairman SHELBY. How confident are you today of your ability to ensure that the Fair Credit Reporting Act and Gramm-Leach-Bliley are being complied with in view of everything that has happened?

Mr. MCGUFFEY. I am confident, Senator, that we have complied with those laws and will continue to be diligent in assuring that the customers that we do credential are credentialed at a high standard and in fact have instituted new procedures and will be instituting additional procedures such as site inspections for those customers who have access to personally identifiable information.

Chairman SHELBY. Mr. Hendricks, I have a couple of questions for you, if you would.

Mr. McGuffey indicated that ChoicePoint conducts audits to ensure that its customers are in compliance with the applicable laws governing information use, the ones I cited. Who has the strongest interest in making sure that those laws are followed? ChoicePoint, the firm trying to obtain the information, or the consumer to whom the information relates?

Mr. HENDRICKS. I think the consumer has the strongest interest in ensuring the privacy, accuracy, security of their data, because if something goes wrong with their data——

Chairman SHELBY. It could be very hurtful, could it not?

Mr. HENDRICKS. Yes, they are the ones sitting at the bottom of the driveway, and all the stuff comes down their way. The main damage from identity theft is all that bad stuff goes on your credit report, and as this Committee knows, it takes a long time to get it off. I am concerned that ChoicePoint and a lot of companies, a lot of database companies, they do not audit for the accuracy of their information from a consumer privacy accuracy point of view. There is no independent audit, not even Arthur Andersen. I mean, it is a very insular process, and sunshine is the best disinfectant.

Chairman SHELBY. Last year, Derek Smith, the Chief Executive Officer of ChoicePoint, said that if they were going to be viewed as the most admired information company in the world, they were going to have to, using his words, "win the battle of trust." After what has happened, what is ChoicePoint in particular and the information brokerage industry in general going to have to do to deserve a modicum of public trust?

Mr. HENDRICKS. I think they are going to have to show that they can work with this Committee to establish fair information practices in law, as we have, the same kinds of rights we have with the Fair Credit Reporting Act and show they can comply with those rights and to bring transparency to their business, and that is going to be a long, hard haul, and that is why it is going to take them possibly years to get trust back for their entire sector.

Chairman SHELBY. I appreciate your coming today, especially after the break of the hearing the other day. We will continue to pursue these questions, because I am not sure they are going away.

Mr. HENDRICKS. No, we do not know where they are going, but we know they are not going away.

Chairman SHELBY. We thank the panel for your appearance and your participation today.

[Whereupon, at 11:44 a.m., the hearing was adjourned.]

[Prepared statements supplied for the record follow:]

PREPARED STATEMENT FOR SENATOR WAYNE ALLARD

I would like to thank Chairman Shelby for holding this timely hearing on identity theft and recent developments involving the security of sensitive consumer information.

Of more than one million complaints the Federal Trade Commission received in 2001, 86,680 of them were identity fraud complaints. Furthermore, the Government Accountability Office reports that identity theft has been steadily increasing in recent years, based on data provided by credit reporting agencies.

Mr. Chairman, I was shocked to hear that personal information on approximately 1.2 million Federal Government charge cards was lost in transit to a data-storage facility. I am very concerned to hear about all of the time, energy, and effort that consumers involved in this situation have had to put forth in order to protect their information from being misused, abused, and potentially stolen.

I will be particularly interested to hear about what specific steps Bank of America is taking to help protect their customers' identities after the loss of these tapes. By steps, I do not mean a form letter about common sense procedures that a customer can follow in order to protect his or her identity. I mean specific procedures a customer can take, with Bank of America's help, to protect their personal information and identity in this specific circumstance.

In an event such as this, the burden should fall on the entity that made the error—not on the consumer who is entirely helpless and powerless. I have heard from my constituents, and unfortunately this has not been the case, with the burden falling almost entirely on the customer. I will be very interested to hear today how the investigation is proceeding, but more importantly, what Bank of America is doing in the mean time to help the customers involved.

I also look forward to hearing about the 145,000 people whose consumer information was purchased by scam artists from ChoicePoint, and the steps that have been taken to safeguard against this occurrence being repeated in the future.

Again, Chairman Shelby and Ranking Member Sarbanes, I appreciate your attention to this important matter, and look forward to learning what these companies are doing to insure the protection of their customers, as well as determining whether or not the current law provides the necessary protections to consumers.

PREPARED STATEMENT OF EVAN HENDRICKS

EDITOR AND PUBLISHER, PRIVACY TIMES

MARCH 15, 2005

Mr. Chairman, Ranking Senator Sarbanes, distinguished Members, thank you for the opportunity to testify before the Committee. My name is Evan Hendricks, Editor and Publisher of *Privacy Times,* a Washington newsletter since 1981. For the past 27 years, I have studied, reported on, and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications, and Government records. I have authored a book about credit scoring and credit reporting, as well as books about general privacy matters and the Freedom of Information Act. I have served as an expert witness in Fair Credit Reporting Act and identity theft litigation, and as an expert consultant for government agencies and corporations.

I was closely involved in the multiyear process that resulted in the 1996 Amendments and 2003 Amendments to the Fair Credit Reporting Act. Working with your highly competent staffs, I was proud of our many accomplishments in 2003.

The recent ChoicePoint and Bank of America incidents underscore that we have much more work to do in order to ensure Americans' rights to information-privacy.

I think that there is broad agreement that an important lesson to be drawn from our FCRA work is that the best way to improve our national credit reporting system is to strengthen protections for consumers. The more power that consumers have to maintain reasonable control over their credit reports, the better the chances for improving their accuracy and ensuring they will be used fairly and only for permissible purposes. What is true for credit reporting is true for the other noncredit systems filled with personal information.

What is starkly clear from the ChoicePoint episode is the lack of transparency regarding the personal data collected, stored and sold by ChoicePoint and its "cousins," which include Acxiom, LexisNexis/Seisent, and Westlaw—to name a few. Most people do not know about these companies, even though they maintain personal data on over 100 million people.

Moreover, these companies often do not allow individuals to access their data or correct errors—even though other companies and Government agencies could buy the same information data and use it for making decisions about those individuals.

In essence, these are "secret files." In being the first Federal body to articulate Fair Information Principles, the first principle set forth by the 1973 HEW Secretary's Advisory Committee On Automated Personal Data Systems was: "There must be no personal data recordkeeping systems whose very existence is secret." This is because history has shown us that secret files are a recipe for inaccuracy, abuse of privacy, and poor security.

In my opinion, the noncredit database companies generally operate in violation of principles 2–5 as well, at least in regard to information not already covered by the FCRA. Those principles are: (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Possible Solutions

There are no quick or easy solutions to protecting privacy. Like many privacy and consumer experts and advocates, I heartily endorse the concepts underlying legislation introduced by Sen. Bill Nelson and Rep. Edward Markey to extent the protections of the FCRA to noncredit database companies. Similarly, I conceptually favor Sen. Dianne Feinstein's efforts to make notification of security breaches the law of the land. Were it not for the pioneering Californian State law, we might not even know about the ChoicePoint debacle. On the other hand, it would probably be counterproductive for Congress to pass a law that was not at least as strong as the California law. I also agree with the general thrust of measures to curb trafficking in Social Security numbers by Rep. Clay Shaw and others. Details are always important, but since this is not a strictly legislative hearing, we do not need to get into them now.

I also want to bring to the committee's attention the fine work of some of my colleagues, including Consumer Union's endorsement of the efforts of Sen. Nelson/Rep. Markey;[1] the newly drafted "Model Regime For Privacy Protection," by George Washington Univ. Law Prof. Daniel J. Solove & Chris Jay Hoofnagle, head of the San Francisco office of the Electronic Privacy Information Center (EPIC);[2] U.S. PIRG's emphasis that any legislation (1) should be based on FIP's, (2) should have a private right of action, (3) should not preempt States.[3] In addition, Linda Foley of The Identity Theft Resource Center pointed out that when there are security breaches, consumers should not only be notified, but should also be advised as to what information fields were stolen or acquired illegally. And, the Center for Democracy and Technology reminds us not to forget about the oft-overlooked problem of Government access to private sector data.[4]

Because there is so much that we *do not know* about the ChoicePoint and Bank of America incidents, it is premature at this point to identify all of the appropriate responses. That is why my recommendations include a call for a thorough investigation of each incident and a public airing of the results. At the end of the day, I favor Congress taking as comprehensive approach as is politically possible.

Current Gaps In Law, Policy, and Information Systems

The recent incidents underscore gaps in current law, policy and information systems. In its recent exchange with EPIC, ChoicePoint acknowledged that its insurance, employment background and tenant screening "products" were covered by the FCRA. But it argued that the rest of the data, including those sold to law enforcement, were not covered by FCRA. This is particularly troubling given that, as noted in Robert O'Harrow's book, "No Place To Hide" (Free Press 2005), ChoicePoint effectively bills itself as a private intelligence service.

I probably disagree with ChoicePoint's view that so many of its information products fall outside of the FCRA. The Act's definition is intentionally very broad, and

---

[1] *http://www.consumersunion.org/pub/core*_financial_services/002028.html; asking for strong Federal standards for security, customer screening, and consumer access and correction.

[2] *http://papers.ssrn.com/sol3/papers.cfm?abstract*_id=681902.

[3] *www.pirg.org/consumer/pdfs/pirgendorsesnelsonmarkey.pdf.*

[4] *www.cdt.org.*

includes "character, general reputation, personal characteristics, or mode of living . . ." However, the fact that ChoicePoint takes this position means that consumers cannot be assured that they can see and ensure the accuracy of data about them.

Even where ChoicePoint agrees that its products are covered by the FCRA, there are troubling loopholes.

For examples, ChoicePoint says it has three "products" that are free under the FACT Act: the C.L.U.E. (auto and homeowners insurance); "WorkPlace Solutions" (employment background screening) and "Tenant History" (apartment rentals).

ChoicePoint said there would be no C.L.U.E report on you if you have not filed an auto or home insurance during the last 5 years.

However, it also said it would not have an employment history or tenant history report "if you have not applied for employment with a customer that we serve," or "have not submitted a residential lease application with a customer that we serve."[5]

How could it not have a "report" on you, but then sell one to an employer or landlord when they asked for it? Under ChoicePoint's interpretation, you apparently could not check the accuracy of a report before it was sold to a landlord or employer. But the FCRA requires that every CRA shall, upon request, disclose to the consumer "all information in the consumer's file." And, even if no insurance claims were filed, ChoicePoint regularly buys data from State Departments of Motor Vehicles, which presumably means it maintain records on most American drivers in one or more of its databases.

Absent Congressional action, this fundamental question of access might have to be decided by the courts. But that could take years, which is one more reason that Congress should require by law that database companies comply with Fair Information Principles, and give individuals the ability to enforce their rights.

The Gramm-Leach-Bliley Act includes safeguards for the security of credit data, including credit header data (identifying information from credit reports). But if ChoicePoint files are based on identifying information from public records or other noncredit files, then ChoicePoint presumably would argue that it is not subject to GLB's security safeguards.

Under this reasoning, the coverage may be even scantier for other database companies, including Acxiom, LexisNexis/Seisint, and Westlaw.

One of the many ironies is the secrecy shrouding these and other database companies that traffic in consumer data. Accordingly, to adequately protect privacy we need to have greater disclosure about all aspects of their operations and practices. This should not be surprising. After all, the same Supreme Court Justice, Louis Brandeis, called privacy, "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." Brandeis also said "the Sunshine is the best disinfectant."

Privacy Protection Requires "Sunshine"

The truth is that we do not know:

- Precisely what information these companies; collect
- Where they collect it from;
- The manner in which they organize and/or maintain it;
- The mechanisms they have to ensure security, or to facilitate both consumer access to their data and correction of errors (if any);
- Whether they audit their systems to ensure accuracy or take other steps to do so;
- The mechanisms (if any) for notifying consumers if data are leaked.

In the ChoicePoint matter, we do not know precisely how the fraud ring exploited weaknesses in the company's systems. It appears that the thieves used ChoicePoint as a "portal" for accessing credit report data. Equifax told the *Atlanta Business Journal* that as many as 8,000 of its credit reports may have been obtained fraudulently through ChoicePoint.

- Is the 8,000 number accurate?
- Why then did ChoicePoint send notices to 145,000 people? How did ChoicePoint calculate that number and why the discrepancy with the Equifax number?
- Did the fraud ring engage in some two-step process, using ChoicePoint to first try and identify a universe of good candidates for identity theft, and then zero in on the best candidates and pull their full credit reports?
- How long had this been going on?
- Why did not ChoicePoint or Equifax notice what might have been an unusual pattern?

[5] *www.choicepoint.com/factact.html,* visited March 13, 2005.

Needed: A Complete Accounting of The ChoicePoint Case and The Overall Landscape

The unanswered questions cited above underscore the need for a full accounting, not only of the specifics of the ChoicePoint case, but of the overall landscape. Because of the need to maintain the integrity of the ongoing investigations, the various law enforcement authorities are not likely to fully inform the public of what they learn. Therefore, it is imperative that Congress ensure that we have a full accounting of the affair.

More broadly, the time has come for a full accounting of the large database companies and the personal information they collect, maintain, and disclose.

ChoicePoint, Acxiom, LexisNexis/Seisint, Westlaw, and the like should move promptly to disclose publicly the following inventories:

- The Government agencies—Federal, State, and local—that provide them with personal data and under what terms;
- The kinds of personal data they collect;
- The manner in which personal data are housed. To what extent is information from different sources co-mingled? Are there separate "silos?";
- Warranty card information—which database companies collect this, what are their sources, how is it stored and used?;
- 800-toll-free profiling data—consumers can give up personal information about themselves simply by calling well-equipped 800 phone numbers. The information that is captured by a Caller-ID type technology known as Automatic Number Identification (ANI) is stored and sold by some database companies.

State Agencies Should Suspend Sale of Some Personal Data Until Truth Be Known

Considering there remain many "unknowns" concerning the ChoicePoint episode in particular, and the database industry in general, it would seem prudent for some governmental agencies to suspend their release of at least some personal data to ChoicePoint until there is a full accounting.

There simply is no way of assessing the risk to consumers' privacy until we know the answers to the questions listed above. Therefore, it would be imprudent for agencies like State Depts. Of Motor Vehicles to continue to permit the possibly undersupervised sharing of drivers' data with ChoicePoint until confidence is restored. Curbing the release of such data would help reduce the risk of breaches in the near-future, and could also expedite industry cooperation in establishing more robust consumer protections.

"Self-Regulation Already Failed"

Several database companies attempted to show that consumers did not need legal rights by "self-regulating." With much fanfare in 1997, some of them joined with the FTC to announce the "IRSG Principles" (Individual Reference Services Group).[6] While it seemed to offer some promise at the time, in hindsight the effort turned out to be little more than a public relations exercise designed to stave off Congressional action. Many of the FTC's privacy-related recommendations were not followed by industry.

ChoicePoint Wants Benefits, But Not Responsibility

ChoicePoint has been involved in various episodes relating to either improper collection of information or providing inaccurate information that unfairly disadvantaged individuals.

Prior to the 2000 George Bush-Al Gore Presidential battle, Florida-based DBT Online Inc. signed a $4 million contract with the State of Florida to "cleanse" voter rolls of convicted felons. DBT, later acquired by ChoicePoint, had misidentified 8,000 Floridians as felons, temporarily barring them from voting. In July 2002, ChoicePoint settled out of court with the NAACP, which had sued on behalf of the voters. The company recently disputed charges by the Electronic Privacy Information Center that it was responsible for the incident.

"Simply put, ChoicePoint played no role in the Florida election in 2000. Database Technologies (DBT) performed the legally mandated review of Florida's voter rolls prior to our acquisition in 2000. The process, a part of which included DBT, was created by the Florida legislature and implemented by State election officials. DBT was hired to create an overly inclusive list of potential voter exceptions based on criteria established by the Secretary of State, which DBT told the State might create false positives. County election supervisors—not DBT—were solely responsible for verifying the eligibility to vote of any voter identified by DBT on the exceptions

[6] *http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.*

list. In particular, county election supervisors—not DBT—were solely responsible for the decision to remove any voter from the rolls," wrote CEO Derek Smith in a statement posted to the company website.

Here are some other incidents:

- In 2000, ChoicePoint was accused of breaking its contract with the Pennsylvania Department of Transportation for posting drivers' records on the Internet. The State fined ChoicePoint $1.3 million and made the company agree to provide driver information only to insurance companies for insurance-related purposes. The State also barred the ChoicePoint employees involved in the posting from having any association with Pennsylvania records. (see *Privacy Times,* Vol. 20 No. 2, 1/19/00)
- A pending lawsuit accuses the company of violating the Federal Drivers Privacy Protection Act by selling DMV data without drivers' consent (see *Privacy Times,* Vol. 23 No. 13, 7/1/03). ChoicePoint said in SEC filings that an unfavorable outcome in such a case "could have a material adverse effect on the company's financial position or results of operations."
- Also in 2003, ChoicePoint announced it would end its practice of obtaining and selling personal data on Mexican citizens for purposes of verifying identity and citizenship once the person was in the United States. The information—name, address, date of birth, and citizen indentification number—was purchased by the Georgia-based company under a contract that required the vendor to certify the information was legally obtained and was available to be used for identity. ChoicePoint's Chuck Jones told the media that the company agreed to stop the practice because the results of a government inquiry determined the information was confidential under Mexican law. He said the data would be returned to government representatives and purged from the company's system. In April 2003, the AP reported that the U.S. Government had bought access from ChoicePoint to data on hundreds of millions of residents of 10 Latin American countries—apparently without their consent or knowledge. The information allowed a myriad of Federal agencies to track foreigners entering and living in the U.S. (see PT, Vol. 23 No. 13, 7/1/03).

  The same year, a Federal judge in Kentucky ordered ChoicePoint to pay single mom Mary L. Boris $447,000 in punitive and actual damages for violating the Fair Credit Reporting Act by failing to corrected inaccurate insurance claims data after it was disputed. "ChoicePoint's witnesses made particularly negative impressions upon the jury," Judge John Heyburn II wrote. "They repeatedly denied making any mistakes and instead seemed to blame all defective data on others. Furthermore, ChoicePoint employees appeared slow to recognize problems even once they were put on notice and disclaimed all responsibility . . . Most notable, they seemed annoyed at even having to appear at trial. . . ChoicePoint never really explained the computer glitches which apparently caused this problem. To this day, the court is still unclear what procedures, if any, ChoicePoint uses to (e)nsure the accuracy of its mass-circulated reports."
- In two separate cases in 2003, ChoicePoint settled out of court with Louisianans Deborah Esteen and Dorothy Moten Johnson for allegedly selling false information about them to potential employers, according to the *Atlanta Business Journal* and MSNBC. Johnson's background check supposedly revealed she was convicted of public payroll fraud. According to her suit, she had never been arrested or convicted of anything in her life.

Anyone can make mistakes. But what is most troubling about some of these incidents is what appears to be ChoicePoint's consistent unwillingness to take responsibility for them.

Moreover, a new article by Bob Sullivan at MSNBC found that two privacy activists who were able to review their ChoicePoint "general" file found many inaccuracies. For Deborah Pierce, one notation suggested a "possible Texas criminal history" and then recommended a manual search of Texas court records. Pierce had only been in Texas twice and never had a problem with police. There were also numerous inaccuracies in her past addresses and other routine data. The report also listed three automobiles she never owned and three companies listed that she never owned or worked for.

Richard Smith's dossier had the same kind of errors as Pierce's. His file also suggested a manual search of Texas court records was required, and listed him as connected to 30 businesses which he knew nothing about.

It also said that he and his wife had a child 3 years before they were married, that he had been married previously to another woman, and most absurd, that he had died in 1976. "Pretty obviously the data quality is low," Smith said. He equated a ChoicePoint report to the results of a Google search on a person—solid informa-

tion is mixed in with dozens of unrelated items. The more common a name, the more extraneous information is produced.

These descriptions raise troubling doubts about ChoicePoint's methods for collecting data and ensuring accuracy.

Comprehensive Approach is Needed

As U.S. PIRG pointed out, Congress needs to fashion legislation that is based upon principles of "Fair Information Practices" (FIP's). Earlier, I mentioned the five principles developed by the 1973 HEW Task Force.

The Committee should also be guided by the 1980 FIP's developed by the Organization of Economic Cooperation and Development (OECD), with the endorsement of the U.S. Government, Japan, and Western European governments. These eight principles are often referred to as the "Gold Standard" of privacy.

(1) Collection Limitation.
(2) Data Quality.
(3) Purpose Specification.
(4) Use Limitation.
(5) Security Safeguards.
(6) Openness.
(7) Participation.
(8) Accountability.

As mentioned before, the newly drafted "Model Regime For Privacy Protection," by Prof. Daniel J. Solove & Chris Jay Hoofnagle offers even more specific guidance for the issues before the Committee. They are:

Notice, Consent, Control, and Access

1. Universal Notice.
2. Meaningful Informed Consent.
3. One-Step Exercise of Rights.
4. Individual Credit Management
5. Access to, and Accuracy of Personal Information.

Security of Personal Information

6. Secure Identification.
7. Disclosure of Security Breaches.

Business Access to and Use of Personal Information

8. Social Security Number Use Limitation.
9. Access and Use Restrictions for Public Records.
10. Curbing Excessive Uses of Background Checks.
11. Private Investigators.

Government Access to and Use of Personal Data

12. Limiting Government Access to Business and Financial Records.
13. Government Data Mining.
14. Control of Government Maintenance of Personal Information.

Privacy Innovation and Enforcement

Effective Enforcement of Privacy Rights

Mr. Chairman, thank you again for this opportunity. I would be happy to answer any questions and look forward to working with this Committee and others to fashion a solution to the problems raised by these recent data leakages.

PREPARED STATEMENT OF BARBARA DESOER

GLOBAL TECHNOLOGY, SERVICE AND FULFILLMENT EXECUTIVE, BANK OF AMERICA

MARCH 8, 2005

Chairman Shelby, Senator Sarbanes, Committee Members, good afternoon. I am Barbara Desoer, Global Technology, Service & Fulfillment executive for Bank of America. I am a member of Chairman and CEO Ken Lewis' executive leadership team.

On behalf of the leadership of our company and all Bank of America associates, thank you for the opportunity to appear before this Committee to provide our perspective on recent events involving our Government charge cardholders.

I would like to express how deeply all of us at Bank of America regret this incident. We collectively make our living and pursue our professional mission by helping people at home, in business, and in Government manage their financial lives. This work rests on a strong foundation of trust, more so in today's incredibly complex and fast-moving world of electronic commerce than ever before. One of our highest priorities, therefore, is building and maintaining a track record of responsible stewardship of customer information that inspires our customers' confidence and provides them peace of mind.

In my opening remarks today, I will provide an overview of:

- What we know regarding the loss of our computer data backup tapes;
- The steps we have taken to alert and protect our Government charge cardholders;
- Our current information security practices; and,
- Our thoughts regarding new legislation or regulations to improve the security of personal information in our country.

On February 25, 2005, Bank of America began proactively communicating to U.S. General Services Administration (GSA) SmartPay® charge cardholders that computer data backup tapes were lost during transport to a backup data center. The missing tapes contained customer and account information for approximately 1.2 million Government charge cardholders. The actual data on the tapes varied by cardholder, and may have included name, address, account number, and Social Security number.

The shipment took place on December 22, 2004. A total of 15 tapes were shipped. Five were lost in transit. Two of the lost tapes included customer information; the remaining three contained nonsensitive, backup software.

Backup tapes such as these are created and stored at remote locations as a routine industry contingency practice in the case of any event that might interrupt our ability to serve our customers. This is standard industry practice, and is designed to protect businesses, their customers, and the U.S. economy at-large, in the event of disruptions in the economic environment that arise from either natural or man-made causes. Such contingency planning is a fundamental part of our enterprise risk management program.

As is our standard practice, none of the tapes or their containers bore any markings or information identifying our company, the nature of their contents, or their destination. Nor are any of the personnel involved in the shipping process aware of the nature of the materials being shipped. As to the tapes themselves, sophisticated equipment, software and operator expertise are all required to access the information. In addition, specific knowledge of the manner in which the data is stored—that is, the "fragmented" nature of the data and the steps required to reassemble it—would be required.

After the tapes were reported missing, Bank of America officials notified appropriate officials at the GSA. Bank of America officials also engaged Federal law enforcement officials at the Secret Service, who began a thorough investigation into the matter, working closely with Bank of America.

Federal law enforcement initially directed that to preserve the integrity of the investigation, no communication could take place to the public or the cardholders. Doing so would have drawn enormous public attention to the tapes at a time when their whereabouts were still a matter of intense investigation and the specific content was still being analyzed. While the investigation was moving ahead, we put in place a system to monitor the affected accounts and, in fact, researched account activity retroactively to the date of the data shipment to identify any unusual or potentially fraudulent activity in the accounts.

The investigation, which continues today, included a detailed review of the entire transit process for the shipment including the archive vendor, truck drivers, airline personnel, and Bank of America employees. The Secret Service has advised us and GSA management that their investigation has revealed no evidence to indicate that the tapes were wrongfully accessed or their content compromised. The Secret Service findings are complemented by the Bank of America fraud monitoring process which continues to indicate there has been no unusual activity or attempted unauthorized use of the monitored accounts to date.

In mid-February, law enforcement authorities advised us that communication to our customers would no longer adversely impact the investigation. We have completed the initial notifications and are continuing to communicate to our customers to ensure they understand additional steps we are taking to help protect their personal information.

Bank of America quickly established a toll-free number Government charge cardholders could use to call with questions or request additional assistance. We also have offered credit reports and enhanced fraud monitoring services to cardholders

at our expense. In an effort to be extra cautious and open with our customers, we also communicated to Government cardholders whose account information was not included in the lost tapes.

Government cardholder accounts included on the data tapes have been and will continue to be monitored by Bank of America, and Government cardholders will be contacted should any unusual activity be detected. No unusual activity has been observed to date. Per standard Bank of America policy, Government cardholders will not be held liable for any unauthorized use of their cards.

In 2002, the Treasury Department chose our company to establish and chair the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. We also are a member of the President's National Security Telecommunications Advisory Committee, which provides subject matter expertise to study issues vital to advancement of national security and emergency preparedness.

I mention this evidence of our leadership not simply to highlight our accomplishments. We all agree this is a time for humility, and we have come here in that spirit. Rather, I wish only to demonstrate to the Committee the seriousness with which we regard these issues and the gravity with which we regard our responsibility for leadership.

Without a strong foundation of trust and confidence, our industry cannot function and cannot serve our customers. We understand all too well this fact and its implications for our business, our economy, and our country.

Our information security standards are based on regulatory guidance from the Federal Government (such as the OCC, the FRB, and others) and international banking regulatory bodies. In addition, the bank's strategy includes a continuous review of information security assessment criteria used by industry information security professionals. It is the bank's goal to meet or exceed information security standards and regulations dictated by our regulators or used by our industry peers in our day-to-day operations.

In that spirit, I would like to provide a brief overview of our Corporate Information Security Program. The Bank of America Corporate Information Security Program is designed to:

- Develop and implement safeguards for the security, confidentiality, integrity, and availability of customer information;
- Achieve protection of information against threats to security based on the value of the information or the harm that could result to a customer from unauthorized access;
- Monitor and respond to attempts to threaten the security of customer information;
- Develop and implement plans to provide backup systems to prevent information damage or destruction caused by environmental hazards or malicious actions; and,
- Adjust the Bank of America Corporate Information Security Program in response to changes in technology, information sensitivity, threats, or the business environment.

As a national financial institution, we are highly regulated and regularly examined on our practices regarding security of customer information. We are required to follow specific regulatory guidance from the Office of the Comptroller of the Currency on how to handle such information. And we are constantly working to enhance the systems we use to monitor customer data to ensure that we know where that data is and how it is being used.

The incident we are discussing was unfortunate and regrettable. That said, we feel that it has shed helpful light on a critical element of the industry's practices for data transport. We view this as an opportunity to learn and to lead the industry to better answers that will give our customers the confidence and security they deserve.

As I said earlier, we decided, out of an abundance of caution, to notify the affected accountholders after law enforcement advised us that notification would no longer adversely affect the investigation. However, we also acknowledge that providing notices when there is low risk that the information will be misused has potential drawbacks, such as creating unnecessary anxiety in customers, and if provided too frequently in non-threatening situations, degrading the effectiveness of a security breach notice.

Proposed Federal legislation would require that customers be notified immediately whenever a security breach is discovered. Our recent actions demonstrate our support of the conviction that customers have a right to know when their information may have been compromised, and that timely notification in the appropriate circumstances could help to minimize various risks associated with a compromise of customer information.

At the same time, we advise some caution regarding legislative solutions. For example, in some instances a thorough investigation of the security may conclude there is no risk that the information was used for illegal purposes. In these instances, it is probably best to leave it to the discretion of the institution to decide if customers should be notified.

Bank of America's participation in and leadership of public-private partnerships to advance the cause of information security in this country is clear. We have always maintained that both Government and industry have a role to play, and we have leveraged these working relationships over the past several years with extremely positive results.

That said, in our experience, often the best solutions arise out of the work we do together, but are implemented through the voluntary cooperation of private sector organizations. This is because the information security environment is by its very nature so fluid and rapidly evolving. The environment demands solutions and countermeasures that can evolve and advance with speed and flexibility, in contrast to the more static nature of purely legislative or regulatory solutions.

Members of the Committee, I would like to conclude by emphasizing how much all of us at Bank of America deeply regret this unfortunate incident. The privacy of customer information is one of the highest priorities at our company, and we take our responsibility for safeguarding it very seriously.

I can assure you on behalf of our leadership team and all our associates, we will do all we can to ensure that our customers have the freedom to engage in business and commerce and manage their financial lives secure in the knowledge that their personal information will be respected and protected by the institutions in which they place their trust.

This concludes my prepared testimony. I will now be happy to answer any questions.