ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION

HEARING

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 4, 2005

Printed for the use of the Committee on Financial Services

Serial No. 109–23

U.S. GOVERNMENT PRINTING OFFICE

24–091 PDF WASHINGTON : 2005

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
RICHARD H. BAKER, Louisiana
DEBORAH PRYCE, Ohio
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LaTOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, Jr., North Carolina
JUDY BIGGERT, Illinois
CHRISTOPHER SHAYS, Connecticut
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona
JIM GERLACH, Pennsylvania
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
MICHAEL G. FITZPATRICK, Pennsylvania
GEOFF DAVIS, Kentucky
PATRICK T. McHENRY, North Carolina

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, Jr., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
CAROLYN McCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
MELISSA L. BEAN, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
GWEN MOORE, Wisconsin,

BERNARD SANDERS, Vermont

ROBERT U. FOSTER, III, *Staff Director*

CONTENTS

ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION

Wednesday, May 4, 2005

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The committee met, pursuant to call, at 10:03 a.m., in Room 2128, Rayburn House Office Building, Hon. Michael Oxley [chairman of the committee] presiding.

Present: Representatives Oxley, Bachus, Castle, Kelly, Gillmor, Biggert, Tiberi, Kennedy, Hensarling, Brown-Waite, Harris, Renzi, Pearce, Price, Davis of Kentucky, McHenry, Frank, Maloney, Velazquez, Watt, Hooley, Carson, Sherman, Lee, Moore of Kansas, Crowley, Clay, Israel, McCarthy, Matheson, Lynch, Scott, Green, Cleaver, Bean, Wasserman Schultz, and Moore of Wisconsin.

The CHAIRMAN. The committee will come to order.

This morning the committee meets to consider a topic we have been hearing about on an almost daily basis during the past few months: data security and its connection to the crime of identity theft.

Several recent high-profile security breaches have focused public attention as never before on the vulnerabilities of companies' data security systems. Congress now has to ask: Are we doing enough to protect against the theft and misuse of sensitive commercial information on consumers?

Protecting sensitive information is an issue of great importance for all Americans. In recent years, criminals in the United States and abroad have become increasingly inventive in finding ways to access and exploit information systems in order to commit identity theft.

According to a Federal Trade Commission estimate, over 10 million Americans are victimized by identity thieves each year, costing consumers and businesses over $55 billion per year, not counting the estimated 300 million hours spent by victims trying to repair damaged credit records.

The financial costs are staggering, with over $10,000 stolen in the average fraud.

The Financial Services Committee has worked tirelessly over the past several Congresses to identify and enact solutions to this destructive crime.

During the 108th Congress, over 100 witnesses came before this committee to testify on the reauthorization of the Fair Credit Re-

porting Act. Through that process, under the leadership of the gentleman from Alabama, Mr. Bachus, the committee developed an exhaustive record on the need to increase safeguards designed to protect consumers and businesses alike from identity theft.

Through bipartisan cooperation on this committee, we ultimately produced strong consumer protection in anti-identity theft legislation known as the Fair and Accurate Credit Transactions Act, or FACT Act.

The FACT Act places new obligations on financial institutions to prevent identity theft, entitles consumers to a free annual credit report from each of the three major credit bureaus and creates a national fraud alert system to simplify a consumer's ability to detect and report fraudulent activity.

The FACT Act was signed into law on December 4, 2003, and is currently in the process of being fully implemented by federal regulators in the financial services industry.

The federal banking regulators have also been hard at work on other initiatives to protect sensitive information.

On March 29, 2005, the Federal Reserve, FDIC, OCC and OTS issued final data security standards for depository institutions that are required in Title 5 of Gramm-Leach-Bliley. The standards call for every financial institution to implement a response program to address incidents of unauthorized access to consumer information maintained by the institution and to notify the affected customer as soon as possible.

In light of continuing guidance from the regulators, it is my hope that we can focus today on the broader issue of data security and how best to protect sensitive information from being improperly accessed, and ensure that consumers receive prompt and effective notice when sensitive information has been compromised and is likely to have been misused.

One of my concerns in this regard is that given the dramatic rise in recent reports on data breaches, there will be a headlong rush toward notification in every instance.

When no evidence surfaces to indicate that their information has been misused, consumers may begin to ignore these notices as just that many more pieces of unsolicited junk mail.

California recently enacted legislation requiring disclosure of any data security breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Only a small percentage of these cases, however, have actually resulted in any fraudulent activity.

Other states are considering legislation similar to California's. It is important that this committee take a look at what is being contemplated in the States and consider whether a national breach notification standard will work best for American consumers.

I would like to welcome our witnesses to today's hearing, and I look forward to hearing your testimony and working with you to find ways to prevent future data security breaches and continue our efforts to combat identity theft.

The Chair's time has expired. I now yield to the gentleman from Massachusetts and the Ranking Member.

Mr. FRANK. Thank you, Mr. Chairman.

Before I yield my time to the gentlewoman from Illinois, Ms. Bean, who has been a very energetic person involved in this, I did want to note: I was somewhat pleased to hear you say that there was some concern, and I assume the industry shares this concern, on too much unsolicited junk mail going to individuals.

If they, in fact, the industry is worried about, the financial services industry, about too much unsolicited junk mail going to individuals in this instance, it is a breakthrough, because I have not found them in the past to be terribly sensitive to that. At least my mailbox will welcome this new sensitivity. And I hope it spreads from just notification here to maybe some other areas.

And with that I want to yield to the gentlewoman from Illinois, who has been a real leader in this in her very first few months here.

Ms. BEAN. Thank you, Mr. Frank. I appreciate the opportunity to speak today.

First, I would like to thank you and Chairman Oxley for your leadership on this very important issue of consumer data security.

The recent high-profile data security breaches at ChoicePoint, Bank of America and LexisNexis have continued to fuel ongoing concerns about the safety and security of Americans' personal financial data. These concerns have forced Congress to once again examine how industry and government can work together to better ensure that an individual's private personal information is adequately protected.

As a new Member of Congress and a new member of this committee, I am honored to join in this endeavor. I know that many of my colleagues, particularly Representative Hooley, have worked hard on this issue for many years, and I look forward to working with them as we move forward.

In March, Americans were shocked to learn that the private data—including Social Security numbers, credit files and personal health information—of nearly 150,000 Americans were sold by ChoicePoint to fraud artists posing as legitimate businesses. However, as illustrated by the subsequent data breaches nationwide, the ChoicePoint case was not an isolated incident. In fact, according to the privacy right center, up to 10 million Americans are victims of I.D. theft each year, and these numbers are on the rise.

Even though victims do not usually end up paying their imposters' bills, they are often left with a bad credit report and must spend months and even years regaining their financial health.

In a recent profile of an individual who fell victim to identity theft, the Chicago Tribune explained that these victims often learn the hard way that the crime is like a chronic disease that goes into remission only to stir up again when least expected.

It is not uncommon that for years after an identity theft, victims have difficulty getting credit, obtaining loans, renting apartments and even getting hired by employers.

As the volume of personal data held by corporations, data brokers and business continues to increase, the issue of securing this data and protecting one's privacy takes on particular importance.

To begin addressing this issue, in early March I joined with Representative Maloney and Representative Gutierrez in introducing H.R. 1069, the Notification of Risk to Personal Data Act, or H.R.

1069. It is the companion bill to legislation introduced by Senator Feinstein and is based on the California notification law, with which I am sure you are familiar.

I believe this bill is a good first step and is based upon sound principles. However, I am mindful that even legislation with the best intentions can create unnecessary and unforeseen burdens. We must find a solution that provides consumer protection but is viable and meaningful in its execution.

I am optimistic that this can be done, because I know both consumers, business and Congress sharing a common goal: to keep Americans' personal information secure.

I thank the witnesses for testifying before the committee today, and I appreciate your taking the time to share your thoughts.

I am particularly interested in your testimony as it relates to notification and triggering of notification.

I yield back the balance of my time.

The CHAIRMAN. The gentlelady's time has expired.

The gentleman from Alabama, Mr. Bachus?

Mr. BACHUS. I thank the Chairman.

I think this is a very important issue, and I think the thing, as we go forward, we ought to remember is that there are different kinds of data or different documents. There are financial documents, there are personal documents, there is credit card information, there is even health records—and all of those can be used to some extent to perpetrate identity theft.

Also, that data, sometimes it is stored, sometimes it is disposed of, sometimes the problems are the security in how it is stored, sometimes the problems are how it is disposed of.

And there are different institutions that have it, and different laws that apply to that data storage. The FACT Act sets up one standard, Gramm-Leach-Bliley sets up another standard, HIPAA sets up another standard.

I think, as a result of the high degree of I.D. theft that we have and the different statutes we have, sometimes there are gaps in the statutes where they may or may not cover certain documents.

We do need a national standard. And we need a national standard on notification.

If we do not have that, it is going to be simply impossible for businesses to know what to do or how to comply or know what standard.

I would think that one thing this committee ought to do is look at the existing law. When we come up with legislation, we ought to at least allow the regulators, the FTC, as they have done in the disposal rules, to fashion some parameters and try not to get too immersed in the finite details as we do this.

I want to commend Mr. Castle and Ms. Pryce and others on the other side for pushing this issue.

And I would like to yield the balance of my time to Mr. Castle, who has been a leader in this effort.

Mr. CASTLE. I thank the gentleman very much for yielding and, of course, for all his work in this and many other areas in banking.

It is clear that we do live in a world that is becoming increasingly complicated in relying on technology and dependent on data for instant decisions. Therefore, I believe, Mr. Chairman, it is

worthwhile for us to explore the practicality of requiring data base security and safeguards for most of the public and private sectors, while our financial institutions, as defined by Gramm-Leach-Bliley, are already required to secure their sensitive data. It may be that we should do likewise across other sectors.

In the coming weeks, we are planning to introduce a comprehensive bill that in part requires many more databases to have a standard level of protection.

In addition, we will define what constitutes a breach so that affected entities, regulators and consumers can be notified when appropriate and in a coordinated manner.

I am also pleased to be working with the gentlewoman from Ohio, Ms. Pryce, on this legislation that is intended to adjust a number of these and other concerns.

And finally, I am interested in hearing from our panelists about steps they took to ensure the future safety of the breached parties' sensitive information. Some companies have provided free credit monitoring for all those that were subject to the breach. I think this is an enormously positive step that helps consumers and restores confidence and peace of mind to many.

So we appreciate you being here.

And I appreciate, again, the gentleman yielding.

I yield back to the gentleman from Alabama.

The CHAIRMAN. The gentleman yields back.

The gentlelady from Oregon, Ms. Hooley?

Ms. HOOLEY. Thank you, Chairman Oxley and Ranking Member Frank, for convening this hearing today.

In my opinion, data security is one of the most important issues that will be brought before this committee in the 109th Congress. Its impact is immense. Consumers, businesses, local and federal law enforcement all have a stake in the manner in which we solve the problem created by data security breaches.

I look forward to all of the members that have taken an interest in this, particularly Representative Bean.

I look forward to continuing in a bipartisan manner in which this committee has operated in recent past to build a broad consensus for an effective solution.

Identity theft represents a fundamental threat to e-commerce, our economy, as well as our homeland security. No longer are we facing just hobbyist hackers creating a nuisance. Increasingly these attacks are driven by skilled criminals.

Identity theft is big business. The Federal Trade Commission estimates that 9 million to 10 million Americans are victims of identity theft every year to a total cost to business and consumers approaching $50 billion. For that reason, it is imperative that Congress and the private sector work together to make certain that sensitive personal information is protected by adequate safeguards.

The committee made progress in this respect in the 108th Congress with the passage of the FACT Act, and now we have to build on that success.

This will not be easy. There are many tough questions that need to be answered.

First and foremost among them will be how we notify consumers whose information has been compromised. Under what cir-

cumstances should they be notified about a breach? When a notice of breach is issued, what information should that notice include? What form should a uniform notice of breach take? These are just a couple of the questions that we are going to have to answer.

I am confident that by working together we can find practical solutions that will provide consumers with landmark protections while also avoiding an undue burden on enterprises who possess, for legitimate purposes, very personal information.

I thank you and yield back the remainder of my time.

The CHAIRMAN. The gentlelady yields back.

We now turn to our distinguished panel.

The first witness is Ms. Barbara Desoer, Global Technology, Service and Fulfillment executive from Bank of America followed by Mr. Eugene Foley, president and CEO of Harvard University Employees Credit Union; Mr. Don McGuffey, senior vice president for Data Acquisition and Strategy at ChoicePoint; Mr. Kurt P. Sanford, president and CEO of U.S. Corporate and Federal Government Markets at LexisNexis; and Mr. Bestor Ward, president of Safe Archives-Safe Shredding LLC—which I understand has some Alabama connections, is that right, Mr. Bachus?

Mr. BACHUS. Yes. In fact, Mr. Chairman, I would like to commend Mr. Ward for his testimony. I have read his testimony. He represents the NAID and their membership. They are experts and committed to the proper destruction of paper records and other media containing sensitive information financial or personal nature that is often misused by identity thieves.

Sometimes we sort of focus on people breaking into data storage, but there is a tremendous need for, as these records are disposed of, to have them properly shredded. And we actually, today, have people that actually dive into the dumpsters and get this information and cause a lot of destruction and pain.

I commend Mr. Ward. He is quite an expert on this.

He also is on the board of directors of one of the largest banks in the United States and has counseled them and has become an expert in this field.

Thank you.

The CHAIRMAN. The gentleman from Massachusetts is going to introduce one of our witnesses.

Mr. FRANK. Thank you, Mr. Chairman.

I am very pleased to have Eugene Foley, who is the president and CEO of the Harvard University Employees Credit Union.

The credit union had been speaking with me about problems they have had with regard to breaches of security and the difficult position they have sometimes been put in, vis-a-vis the people who are their credit card holders. They have been caught, I think unfairly, in the middle on some of these cases.

So I would particularly even have them talk about addressing this.

I appreciate Mr. Foley's willingness to accommodate this. The credit union movement in our state as elsewhere, is a very highly regarded one. He speaks for a very important credit union on an issue that I think is clearly of relevance to all financial institutions, not just the credit unions.

The CHAIRMAN. The gentleman from Georgia, Mr. Scott?

Mr. SCOTT. Thank you very much, Mr. Chairman.

I certainly want to take this opportunity to welcome ChoicePoint, Mr. Don McGuffey, for your testimony on this, this morning.

As every member of this committee, we have all been following the challenges at ChoicePoint. I certainly want to take this opportunity to commend ChoicePoint for responding to this challenge. It is a difficult one.

We certainly want to welcome you here today and certainly look forward to your testimony. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. And the gentleman from Georgia as well, Dr. Price?

Mr. PRICE. Thank you, Mr. Chairman.

I wish to associate my comments with Mr. Scott regarding ChoicePoint. They are located in my district. They have been a wonderful corporate citizen, extremely responsible in dealing with the matters that they have been confronted with. I commend them for that and look forward to their testimony.

The CHAIRMAN. We now turn to our distinguished panel—and I probably butchered your name. Is it Desoer?

Welcome to the committee.

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

Ms. DESOER. Thank you very much.

Chairman Oxley, Congressman Frank, 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's direct executive leadership team.

On behalf of leadership of our company and all Bank of America associates, thank you for the opportunity to appear here today before this committee to provide our perspective on the loss of computer backup data storage tapes that were reported by Bank of America earlier this year.

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 them peace of mind.

On February 25, 2005, Bank of America began proactively communicating to the United States General Services Administration 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.

Now, 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 service our customers.

After the tapes were reported missing, Bank of America notified the GSA, and also engaged the Secret Service, which began a thorough investigation into the matter, working closely with our corporate information team internally.

Federal law enforcement initially directed that, to preserve the integrity of the investigation, no communication could take place to the public or the cardholders. While the investigation was moving ahead, we put in place a system to monitor the affected accounts and 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 advised GSA management and us that their investigation revealed no evidence to indicate that the tapes were wrongfully accessed or their content compromised.

In mid-February, law enforcement authorities advised that communication to our customers would no longer adversely impact the investigation.

Following our initial cardholder notifications, we continued to communicate with our customers to ensure that they understood the additional steps we were taking to help protect their personal information and to assist them with any questions they might have.

We established a toll-free number that government charge cardholders could use to call with questions or request additional assistance.

We offered credit reports and enhanced fraud-monitoring services to cardholders at our expense.

Government cardholder accounts included on the data tapes have been and will continue to be monitored by Bank of America, and cardholders will be contacted should any unusual activity be detected.

According to standard Bank of America policy, these cardholders will not be held liable for any unauthorized use of their cards.

The incident 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 the security that they deserve.

Our recent actions demonstrate our belief that our customers have a right to know when there is reason to conclude that their information may have been compromised and that timely notification in the appropriate circumstances could help to minimize any associated risks.

Furthermore, our approach and existing polices and practices also are in accordance with the recently issued Interagency Guidance. We believe this guidance strikes the correct balance with respect to when notification is appropriate and what steps should be taken when a security breach has put a customer's personal information at risk.

In our experience, the best solutions often arise out of the work we do together, implemented through the voluntary cooperation of private sector organizations.

The information security environment, by its very nature, is fluid and rapidly evolving, and demands solutions and counter-measures that can evolve and advance with speed and flexibility.

We look forward to helping promote that speed and flexibility and to taking part in the ensuing legislative dialogue.

Members of the committee, I can assure you that all of us at Bank of America will do everything that we can to ensure that our customers can 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 look forward to answer any questions.

[The prepared statement of Barbara Desoer can be found on page 64 in the appendix.]

The CHAIRMAN. Thank you, Ms. Desoer.

Mr. Foley?

STATEMENT OF EUGENE FOLEY, PRESIDENT AND CEO, HARVARD UNIVERSITY EMPLOYEES CREDIT UNION

Mr. FOLEY. Chairman Oxley, Ranking Member Frank, members of the committee, I would first like to thank you for providing this opportunity for me to speak about the impact of data security breaches on the small-community institutions that issue credit and debit cards.

Harvard University Credit Union is a $200 million organization located in Cambridge, Massachusetts.

Currently there are about 4,600 card-issuing credit unions in this country, supporting over 12.5 million accounts for our members.

I have experience with this issue not only as the CEO of a credit union that had about 700 of our 10,000 card accounts compromised in just one incident last year but also as a recent victim of identity theft myself.

While I was sitting in my office with my own debit card securely in my wallet, my checking account was cleaned out by a series of transactions that happened 3,000 miles away.

Although I had other sources of funds to draw on throughout the process of reestablishing my account balance, this is often not the case for many credit union members and small-bank customers who are living paycheck to paycheck. They cannot afford any interruption in their cash flow.

Given my position, I am particularly responsive in protecting my own sensitive information. But this caution is meaningless when entities that have captured and retained the data contained on the card stripe are careless or not compliant with security standards.

The frequency of large-scale data compromises is increasing, and the smaller card-issuing institutions are struggling to keep up the constant vigilance it takes to immediately react in notifying and crediting our cardholders for their losses.

Within the past 2 weeks alone, we have read of three major breaches which have compromised the accounts of millions of American consumers.

The first large security breach to have an impact on small banks and credit unions came to light last year as a result of hackers stealing a large amount of consumer information from the retailer,

BJ's Wholesale Club. This case exemplifies the merchant in direct violation of card association rules and regulations.

While card issuers are required to fastidiously comply with protecting sensitive account data, the resources they expend in this effort are squandered if merchants are not held to the same standard.

A recent article in the Wall Street Journal cited a $5.7 million lawsuit filed last month against BJ's Wholesale Club by CUNA Mutual Insurance Corporation on behalf of 163 credit union bondholders.

Individual banks have also brought suit for their losses.

These costs include not only the amounts lost to fraud, but also the costs for reissuing and blocking cards, for notifying cardholders and monitoring accounts.

There are card association rules in place regulating how the consumer information, which is imbedded on the magnetic stripe on the back of each card, should be handled. But these rules have proven to both insufficient and laxly enforced.

Absent card association enforcement or legislative redress, banks and credit unions have had to resort to litigation in order to find a remedy for their losses.

The surest way to limit the potential damage when a merchant's files are hacked and a large base of card information is stolen is to cancel the existing cards and reissue new cards. As small banks and credit unions hold a close relationship with their cardholders, this is most often the action that they take. It is costly, time consuming and puts a significant strain on the scarce resources we have.

Unfortunately, our best effort to protect our members and customers is often met with another penalty by causing the consumer to question the safety and security of the card issuer rather than the merchant who has inadequately safeguarded their personal information.

This means that in addition to the significant monetary losses, small banks and credit unions are also unfairly exposed to reputation risk as a result of this problem.

Even after a breach has been identified by the merchant, issuing institutions cannot count on getting accurate and timely notification to pass along to the consumer. Most times, the issuer is relying on reports in the media to determine the nature of the breach.

Without accurate information, it is impossible to appropriately inform our members as to how their information was stolen, and they are often left with the impression that the bank or credit union is at fault.

While we have had the benefit of seeing the California law requiring disclosure of security breaches in action for nearly 2 years, and their experience offers us some guidance, there is room for improvement.

It is our hope that the committee will put its authority and energy behind initiatives that will require the major card companies to notify financial institutions immediately in a format that is usable for the affected issuer. That information should include: when a breach occurred, which merchant is responsible for that breach and what accounts are affected.

It should also detail what type of personal information was compromised.

Specifically, any new statute would benefit from explicit definitions. For example, clarity with regard to which businesses would be covered, along with what constitutes personal information, are areas where the California statute has been questioned.

A particular concern is an exclusion that the California law provides for encrypted data. Unfortunately, advances in hacking seem to match advances in encryption, and those that can breach credit files are quite likely to be able to gain access to decryption technology.

In addition, to ensure that all consumers have the utmost protection from this insidious threat, we believe that as a best practice all issuers should be required at a minimum to inform consumers when their account has become compromised and their personal financial information has been stolen. These consumers should then have the right to determine if they wish to have their cards canceled and reissued in a timely fashion at no cost to them.

Mr. Chairman and members of the committee, thank you for affording me this opportunity.

[The prepared statement of Eugene Foley can be found on page 69 in the appendix.]

The CHAIRMAN. Thank you, Mr. Foley.

Mr. McGuffey?

STATEMENT OF DON MCGUFFEY, SENIOR VICE PRESIDENT, DATA ACQUISITION, CHOICEPOINT INC.

Mr. MCGUFFEY. Chairman Oxley, Ranking Member Frank and members of the committee, good morning.

I am Don McGuffey, senior vice president for Data Acquisition and Strategy of ChoicePoint. I have been with the company since its inception in 1997.

ChoicePoint has previously provided Congress with testimony about the recent improper data access and the criminals who perpetrated this fraud, the steps we are taking to protect affected consumers and the measures that we are taking to prevent similar violations from occurring in the future.

While I have described the company's actions in my written statement to the committee, I would like to specifically offer a sincere apology on behalf of ChoicePoint to those consumers whose information may have been accessed by the criminals who perpetrated this fraud.

What I hope you see in ChoicePoint is a company that has listened to consumers, privacy experts and government officials, and learned from this experience. Accordingly, we have responded rapidly and in fundamental ways.

We have provided benefits to potential affected consumers that no other information company had done before and that several companies have since emulated, including voluntary nationwide notification, dedicated call centers and Web sites, free three-bureau credit reports and 1 year of credit monitoring at our cost.

We learned that there are few places for consumers to turn for help if their identity is stolen. This alone increases the fear and the anxiety associated with identity theft. For this reason, we have re-

cently formed a partnership with the Identify Theft Resource Center, a leading and well-respected nonprofit organization dedicated exclusively to assisting identity theft victims.

Most importantly, we have shifted our focus to ensure our products and services provide a direct benefit to consumers or to society as a whole. While this has meant exiting an entire market, we decided that consumers' interests must come first.

We have already made broad changes to our products, limiting access to personal identifiable information, and more changes are under development.

Mr. Chairman, before delving into the specifics of various policy proposals, as my letter I had requested, perhaps it would be helpful if I give members of the committee a brief overview of our company, the products we provide and some insight as to how we currently are regulated.

The majority of transactions our business supports are limited and initiated by consumers. Last year we helped more than 100 million people obtain fairly priced home and auto insurance. More than 7 million Americans get jobs through our pre-employment screening services, and we helped more than 1 million consumers obtain expedited copies of their families' vital records: birth, death and marriage certificates.

These transactions were started by consumers with their permission, and they provide a clear, direct benefit to consumers.

Not all of our other work is as obvious, but the value of it is. At a time when the news is filled with crimes committed against children, we are helping our nation's religious institutions and youth-serving organizations protect those in our society who are least able to protect themselves.

Our products or services have identified 11,000 undisclosed felons among those volunteering or seeking to volunteer with children, 1,055 with convictions for crimes against children, 42 of those felons were registered sex offenders.

Consumers, business and nonprofits are not the only ones that rely on ChoicePoint. In fact, government officials have recently testified to Congress that they could not fulfill their mission of protecting our country and its citizens without the help of ChoicePoint and others in our industry.

Last month, ChoicePoint supported the U.S. Marshal Service in Opertion Falcon, which served approximately 10,000 warrants in a single day for crimes ranging from murder to white collar fraud.

Mr. Chairman, apart from what we do, I also understand that the committee is interested in how our business is regulated at both the Federal and State levels.

The majority of our products are already governed by the FCRA and other Federal and State laws, including the recently enacted companion FACT Act, the Gramm-Leach-Bliley Act and the Drivers Privacy Protection Act, as well State and Federal do-not-call and do-not-mail legislation. We believe consumers benefit from these regulations.

While a small percentage of our business is not subject to the same level of regulation, we believe additional regulation will give consumers greater protections.

And finally, I want to state for the record ChoicePoint's position on future regulation of our industry.

We support independent oversight and increased accountability for those who handle personally identifiable information, including public records. This oversight should extend to all entities, including public sector, academic and other private sector organizations that handle such data.

We support a preemptive national law that would provide for notification to consumers and to a single law enforcement point of contact when personally identifiable information has fallen into inappropriate hands, ensuring that the burden of notice follows the responsibility for breach and that consumers do not become desensitized to such notices.

ChoicePoint supports providing consumers with the right to access and question the accuracy of public record information used to make decisions about them consistent with the principles of FCRA. There are technical and logistical issues that we will need to solve, but they are solvable.

We have already taken steps to restrict the display of full Social Security numbers and would support legislation to restrict the display of full Social Security numbers modeling existing law, including GLB and FCRA, which extending those principles to public record information.

We have all witnessed the significant benefits to society that can come with the proper use of information. But we have been reminded, firsthand, the damage that can be caused when people with ill intent access sensitive consumer data.

As a company, we have rededicated our efforts to creating a safer, more secure society. We look forward to participating in continued discussions of these issues and will be pleased to answer any questions that you may have.

[The prepared statement of Don McGuffey can be found on page 73 in the appendix.]

The CHAIRMAN. Thank you, Mr. McGuffey.

Mr. Sanford, welcome.

I might point out that Mr. Sanford's company is located in Dayton, Ohio. Since we had several parochial interests represented in the introductions, I thought I would add that as well.

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

Mr. SANFORD. Thank you, Mr. Chairman.

Chairman Oxley, Ranking Member Frank and distinguished members of the committee, good morning.

My name is Kurt Sanford. I am the president and chief executive officer for corporate and federal markets at LexisNexis.

I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the protection of consumer information.

LexisNexis is a leading provider of authoritative legal, public records and business information. We play a vital role in supporting government, law enforcement and business customers who use our information services for important uses, including detecting

and preventing identity theft and fraud, locating suspects, preventing money laundering and finding missing children.

LexisNexis products are used by financial institutions to help address the growing problem of identity theft and fraud.

In 2004, 9.3 million consumers were victimized by identity fraud. Credit card companies report $1 billion in losses each year from credit card fraud. With the use LexisNexis, a major bank-card issuer experienced a 77 percent reduction in the dollar loses due to fraud associated with identity theft.

LexisNexis products are also used to help prevent money laundering.

We have partnered with the American Bankers Association to develop a tool used by banks and other financial institutions to verify the identity of new customers to prevent money laundering and other illegal transactions.

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

These are just a few examples of some of the important ways in which are products are used by our customers.

While we work hard to provide our customers with effective products, we also recognize the importance of protecting the privacy of the consumer information in our databases. We have privacy policies, practices and procedures in place to protect this information.

Our chief privacy officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong policies to help safeguard consumer privacy.

We also have multi-layered security processes and procedures in place to protect our systems and the information contained in our databases.

Maintaining security is not a static process. It requires continuously evaluating and adjusting our security procedures to address the new threats we face everyday.

Even with these safeguards, we discovered earlier this year some security incidents at our Seisint business, which we acquired last September.

In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. Upon further investigation, we discovered that unauthorized persons, using I.D.s and passwords of legitimate Seisint customers, may have accessed personally identifying information such as Social Security numbers and driver's license numbers.

No personal financial, credit or medical information was involved since LexisNexis and Seisint do not collect that type of information.

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

Based on these incidents at Seisint, I ordered an extensive review of data security activity going back to January 2003 at our Seisint unit and across all LexisNexis databases that contain personal identifying information. We completed that review on April

11 and concluded that unauthorized persons, primarily using I.D.s and passwords of legitimate Seisint customers, may have accessed personal identifying information on approximately 280,000 individuals.

At no point was LexisNexis or Seisint technology infrastructure hacked into or penetrated, and no customer data was accessed or compromised.

We sincerely regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify those individuals. We are providing all individuals with a consolidated credit report and credit-monitoring services.

For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information related to fraudulent activity.

We will also provide them with identity theft insurance to cover expenses associated with restoring their identity and repairing their credit reports.

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

I have included details of these enhancements in my written statement.

I would like to focus the remainder of my time on policy issues being consider to further enhance data security and address the growing problem of identity theft and fraud.

LexisNexis would support the following legislative approaches.

First, we support requiring notification in the event of a security breach where there is a significant risk of harm to consumers. In addition, we believe that it is important any such proposal contain Federal preemption.

Second, we would support the adoption of data security safeguards modeled after the safeguard rules of GLBA.

Finally, it is important that any legislation strike the right balance between protecting privacy and ensuring continued access to critically important information.

Thank you again for the opportunity to be here today to provide the committee with our company's perspective on these important public policy issues. We look forward to working with the committee as it considers these important issues.

[The prepared statement of Kurt Sanford can be found on page 79 in the appendix.]

The CHAIRMAN. Thank you, Mr. Sanford.

Mr. Ward?

STATEMENT OF BESTOR WARD, PRESIDENT, SAFE ARCHIVES-SAFE SHREDDING, LLC

Mr. WARD. Good morning. Thank you, Representive Bachus, for your kind words.

Chairman Oxley, Ranking Member Frank and members of the committee, it is a pleasure to be here.

My name is Bestor Ward. As Representative Bachus noted, I am a member of the National Association for Information Destruction,

or NAID. I am also the president of Safe Archives-Safe Shredding, a business that provides secure records management, media storage and information destruction services in Mobile, Alabama.

NAID is the international nonprofit trade association of the information destruction industry. NAID's mission is to champion the responsible destruction of confidential information by promoting the highest standards and ethics in the industry.

I am honored to appear before you today to discuss the important role that proper information destruction plays in the fight against identity theft.

NAID commends this committee for addressing this critical issue.

As you know, much discussion has recently focused on controlling or limiting the sale or transfer of confidential information. Yet that type of control is undermined when disposal of this information is left unregulated. It simply does not make sense to implement information-transfer controls without ensuring that the same sensitive information is not left out on the curb for anyone to take.

Enormous costs, inconvenience and a sense of violation can be avoided through proper disposal of all documents containing sensitive consumer information.

There are number of laws that help fight identity theft, including the Fair and Accurate Credit Transactions Act, or FACT Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act.

However, the scope of these laws is limited to particular industries and particularly records. For instance, the FACT Act only covers consumer report information. But we know that many other documents can be used to facilitate identity theft.

It is critical that we protect all sensitive consumer information, including Social Security numbers, credit card and bank information, telephone numbers and addresses maintained by any business, whether it comes from a consumer report or whether it comes from any other document.

Accordingly, NAID encourages the Congress to take further steps to enact comprehensive legislation that covers all sensitive consumer information in all industries.

Oftentimes, more regulation is not the answer to our country's problems. However, in this context, NAID believes that it is appropriate for two reasons.

First, the costs of identify theft are enormous. Beyond the billions of dollars in losses to customers and businesses, it is difficult and expensive to capture and prosecute perpetrators of this crime. It is much easier to prevent those crimes of opportunity in the first place by eliminating the criminal opportunities, requiring proper methods of disposal as a simple, low-cost means of prevention.

It makes far greater sense to enact strong laws that prevent so-called "Dumpster divers" and other criminals from accessing sensitive information than to impose a massive burden on the law enforcement community to address a problem after substantial losses have been incurred.

I would like to convey to my single point with an anecdote.

Shortly after Georgia enacted information destruction legislation in May of 2003, NAID received a phone call from an employee of a well-known corporation. The caller asked for a list of Georgia

companies that it could retain to shred documents covered by the state's new disposal requirements.

The caller was located in the company's corporate headquarters outside of the State of Georgia, and our NAID representative offered to send a broader list of NAID member-companies that operate in other states where the company does business. The caller's response was, "Well, no thanks. The other states do not have these shredding laws."

This response highlights the need for strong Federal legislation that closes the gaps between existing laws by requiring all businesses to properly dispose of sensitive personal information that is subject to misuse.

This type of legislation is necessary to ensure that these documents are destroyed before someone's identity is.

Mr. Chairman, thank you for inviting me to participate in this hearing today. I am honored to be here, and I would be delighted to answer any questions that you all may have.

[The prepared statement of Bestor Ward can be found on page 92 in the appendix.]

The CHAIRMAN. Thank you, Mr. Ward.

Thank you to all our panelists. It was I think educational for all of our members, including the Chair.

Let me begin with Mr. Sanford, since you had specifically talked about three tenets of Federal legislation. I wanted to have you highlight that again.

As I understand, it was notification based on a federal preemption; data security based on an amendment to Gramm-Leach-Bliley, or an addition to Gramm-Leach-Bliley; and privacy access balance.

If you could just briefly go over that proposal again.

And then I would like to ask each of the panelists to respond to what Mr. Sanford has proposed.

Mr. SANFORD. Mr. Chairman, on the security question, the safeguards in GLBA, which apply to financial institutions, we would recommend that those safeguards could be applied to the information industry. Again, we are not a financial institution, but we think if safeguards were modeled similarly after the standards that were in GLBA, that would be a very welcome measure for our industry.

The notification question is a much more complex matter. There has been great debate on the trigger, but not much debate, it appears, on whether notice should be made. I think most people would agree that providing notice to individuals or consumers where some sensitive financial, credit, medical or personal identifying information is compromised is a good thing.

The question is, what is the trigger? Do we do that when there is just a breach in a system? Or do you need some evidence that that breach could create some potential harm?

For example, let's say an employee in a company leaves the company and conducts a search the next day. That is an unauthorized access to a system. Should we send a letter to the consumer to say that that employee who left that company conducted a search that next day?

Sometimes people do searches on celebrities. Should we send notices to celebrities each time there is a search done?

So we have recommended that where there is some evidence that the nature of the breach could pose a risk of harm to consumers, similar to what the consumer division in California has talked about in their written guidance, we think that ought to be the triggering event so we do not flood the market with a lot of paper that is then dumped in a trash can.

The CHAIRMAN. Would it be based on a quantitative number of consumers affected?

Mr. SANFORD. I do not think it turns on whether or not there is one consumer or 100 consumers. I think it turns on the facts of the nature of the security breach itself, whether or not—I will give you an example.

If you have a security breach for—somebody has hacked into a system and downloaded records, that is probably indicative of the information getting in the wrong hands.

If you have somebody accessing a system using an anonymizer or a key-stroke virus to get information, that begins to suggest that the reason why that information was obtained may be for illicit purposes.

The CHAIRMAN. And a very sophisticated——

Mr. SANFORD. And sophistication is growing in technology.

So on privacy, our comment on privacy was that this is not about just unfettered access for corporations and institutions to have information, personally identifying information. There needs to be a balance, and we need to protect privacy. I mean, I think that is clear. When GLBA was enacted, there was a concern about protecting the privacy of information when we brought financial and insurance institutions together, and we think that balance has to be there.

Corporations like us should not have unfettered access. We should have responsibilities to have safeguards on our data and not be unconcerned about privacy, which, frankly, I think LexisNexis has been very concerned about for many decades.

The CHAIRMAN. Thank you.

Let me, then, begin with Ms. Desoer and ask you to comment about the suggestions that Mr. Sanford put forth.

Ms. DESOER. Thank you.

We do believe there should be a national approach. As a financial services institution, we of course are subject to Gramm-Leach-Bliley. And in addition, the new Interagency Guidance that has been enacted, we believe embraces the principles that are fairly consistent with what he just described, and that is what we are operating under——

The CHAIRMAN. How many states do they operate in?

Ms. DESOER. Twenty-nine, plus the District of Columbia.

The CHAIRMAN. Thank you.

Mr. Foley?

Mr. FOLEY. I also concur that it is important, as California has put out there, to have the disclosure. The only addition that I would advise to the California statute is that it does not cover encrypted data.

And from a notification standpoint, some sort of standard in terms of which businesses are covered and what the standard would be for notifying the consumer, once the definition of that breach has been maintained.

The CHAIRMAN. Thank you.

Mr. McGuffey?

Mr. MCGUFFEY. Yes. I had testified earlier that we would agree with extending the principles of GLB to companies such as ChoicePoint and others in our industry. Both Mr. Sanford and I are in agreement on that matter in that GLB—we are not a financial institution either, so those principles of security are certainly appropriate.

As far as notice goes, we obviously gave nationwide notice. And so a preemptive law from a nationwide standpoint would be certainly appropriate from our view.

The one provision I think in California law that provides for an exception for public record information should be considered to not have an exception, because there is personal identifiable information within public record information, and we have elected, as a company, to not deliver the full Social Security numbers out of public record information. So I think that that exception should be reviewed and reconsidered.

As far as privacy goes, certainly we are supportive of the privacy legislation associated with the consumer information.

The issue of use of personally identifiable information, frankly, is also complicated because the absence of this information oftentimes will give false positives.

So the ability to use that in proper markets and proper business transactions is needed in order to assure that when an individual is either signing up for an account or is trying to be validated for access to rightful information, oftentimes personally identifiable is the way in which we identify and make sure that that is who they say they are. So that is also an issue that needs to be considered, in my view, in your legislative discussion.

The CHAIRMAN. In your experience, could you describe for the committee an example of a false positive, how that operates?

Mr. MCGUFFEY. Certainly.

One example may be that in bankruptcy information now, the Social Security numbers on bankruptcy data is truncated. And we have a lot of common names in the United States. And we find that it is difficult now to try to associate bankruptcy information with the proper individual.

So in the event that a bankruptcy record is associated improperly, then that may have, obviously, adverse implications on the wrong party. So that may be one simple example.

The CHAIRMAN. Truncated in respect of just using the last four digits of the Social Security number? Or——

Mr. MCGUFFEY. Yes. There is actually a couple different methodologies I think in different industries. And indeed, federal bankruptcy is truncating the first five and displaying the last four, which are a little bit more unique in that number. And then there are other industries that are truncating the last four and only delivering the first five.

The CHAIRMAN. So you would suggest that at some point we try to have some uniformity in that.

Mr. MCGUFFEY. I think uniformity is important. And I also believe that there are markets and there are purposes for which the full Social Security number should be used for matching purposes and not necessarily display.

The CHAIRMAN. And should we mandate that?

Mr. MCGUFFEY. We are, as a company, going through and trying to operate in the current environment where we have inconsistencies, and I think mandating an appropriate set of rules is going to be good for the industry.

The CHAIRMAN. Thank you.

Mr. Ward?

Mr. WARD. Thank you, Mr. Chairman.

We are here on a little different mission today in that we are talking about the ultimate disposal of the information.

Mr. Sanford's operation I think is—I think there are about 150,000 pieces of personal identification that were lost there.

Every day in the United States there are millions of pieces of personal identification that have reached the end of their useful life, and they are just simply disposed of, put in the Dumpster, gotten rid of in an unregulated manner.

What you all did here in this committee you should be commended for in the FACT Act. You all created a set of laws that had in particular the disposal rules that are a great model to use throughout the whole business world. If those disposal rules could be mandated to be used across all businesses for all types of personal information, a lot of the Dumpster-diving issue would go away.

The CHAIRMAN. Thank you.

The Chair's time has expired.

The gentlelady from New York, Ms. Maloney?

Mrs. MALONEY. I am going to yield to Ms. Velzaquez.

The CHAIRMAN. The gentlelady from New York, Ms. Velazquez?

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Mr. McGuffey, how many individuals were affected by the theft of personal information that occurred at ChoicePoint?

Mr. MCGUFFEY. Congresswoman, we notified approximately 145,000 individuals.

We have been working with law enforcement in California in order to continue the investigation. We are not aware today of exactly how many individuals have been the subject of actual identity theft.

Ms. VELAZQUEZ. Yesterday the Wall Street Journal reported that the Los Angeles County sheriff reported that data on millions of people have been downloaded. How do you reconcile your number and that number?

Mr. MCGUFFEY. The comments in the testimony, I think, that the Wall Street Journal reflected on for Detective Decker were comments that were made in the very initial stages of the investigation. They were around the time of the arraignment and the arrest of the individual.

The investigation, having now proceeded over several months, has clarified the view, and it is my understanding after having

even discussions yesterday with our representative, Robert McConnell, that Detective Decker's view is that the number that we have noticed is consistent with his expectation and understanding of the investigation today.

Ms. VELAZQUEZ. Does your company plan to employ, in the future, a way to readily track data that is compromised due to data breaches?

Mr. MCGUFFEY. We do have, today, methods—there are billing logs and transaction logs that we in fact used in the latter part of 2004 and into January to recreate all the various, different searches that the accounts that we identified as being fraudulent.

So we do have methods today. We are looking at our technology in order to try to enable ourselves to be more responsive.

Ms. VELAZQUEZ. Sir, do you believe that companies in this industry should be subject to the highest standard of data security so that we can assure that you are a step ahead of thieves, not a step behind.

Mr. MCGUFFEY. Yes, Congresswoman, we are, ourselves, rededicating our efforts, and we have continuously improved our processes, because as you mentioned, we are trying to stay ahead of the criminals.

Ms. VELAZQUEZ. So you believe that you should be subjected to a high standard?

Mr. MCGUFFEY. Yes.

Ms. VELAZQUEZ. Mr. Sanford?

Mr. SANFORD. Well, we certainly think we need to enhance our security based on what we learned at this company that we acquired.

As I indicated in my opening remarks and my written testimony, we certainly would support the safeguard rules modeled after GLBA. I think that that is the right approach. It imposes a framework that says: Apply your security based on the context and circumstances of what business you are engaging in.

The more we have learned about this, the more we spent time with law enforcement, the more sophisticated we are getting and understanding what the threats are.

Ms. VELAZQUEZ. Mr. Ward?

Mr. WARD. Absolutely, Congresswoman, we do believe in that. Our association has endeavored to try to set itself at the highest standard. We have a certification process that our shredders have to go through, and it is a pretty rigorous set of parameters that we have to go through. I think that as the future unfolds, we will continue to add to that.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

The CHAIRMAN. I thank you.

Mr. Bachus is recognized for 5 minutes.

Mr. BACHUS. I thank the Chairman.

First of all, Mr. McGuffey, is ChoicePoint covered by Gramm-Leach-Bliley, or any of your subsidiaries today? Are they under the data security requirements of that act?

Mr. MCGUFFEY. We are regulated in certain aspects of our company associated with GLB. While we are not a financial institution, to the extent that some of that data is controlled by GLB, then we are required to comply.

Mr. BACHUS. How about the FACT Act or Fair Credit Reporting Act? Are you subject to those data security requirements?

Mr. MCGUFFEY. Yes, Congressman, we are. The majority of our business is governed by the FCRA and also the FACTA.

Mr. BACHUS. How about LexisNexis, Mr. Sanford?

Mr. SANFORD. Congressman, under GLBA, as a recipient of data from a financial institution or a consumer reporting agency, we are subject to the privacy provisions. But as we are not a financial institution, we are not subject to the security provisions. That is why we suggested modeling that.

We have a very small part of our business that is governed by FCRA, for example, some of the employment screening. And that obviously is covered by FACT Act as well.

Mr. BACHUS. And I am not sure, Mr. McGuffey, that ChoicePoint was under the data security requirements of Gramm-Leach-Bliley.

Mr. MCGUFFEY. As not being a financial institution, we are not under the data security, but we——

Mr. BACHUS. Which in—yes, okay.

And I will say this. Right now banks have heavy financial security regulations imposed on them right now. So I think when we engage in this debate or discussion, we have to realize that financial institutions are already under heavy financial data security requirements.

In fact, if you visit a large bank, you see that several of them have $50 million and $60 million facilities that operate 24 hours a day. They are constantly—and it is very interesting that constantly they are interdicting attempts to break into the system almost on an hourly basis. It is incredible to sit there and watch people try to hack into the system.

It is very sophisticated.

I will yield the balance of my time to Mr. Castle.

Mr. CASTLE. [Presiding.] Let me ask one question now, and I will have my own time here in a moment.

But just I guess, Mr. McGuffey and Mr. Sanford, and I think I understood the whole panel basically indicating that we have to go more universal in this and that probably doing it at a national level is the way to go. And I think there is probably general agreement on this.

And by the way, this is legislation which I think we will not have a great political divide on it. It is a question of getting the right language. This is not Republican-or Democrat-type legislation. So hopefully we can work this out.

I have several concerns about the extent of where we should go, and one of them is how wide should the range of businesses be.

Clearly, we have to go beyond the financial institutions. I do not think anybody disagrees with that. I am not sure anybody here has any disagreement with their own business necessarily being included.

But I think of various things that have happened. For instance, I do not know the whole details of—I think it was a GM card where HSBC gave notice and others did not give notice, and the Polo clothing chains were involved in this. I do not know how far we should go with all of this.

Do you have any thoughts about where this should cut off, if at all?

There is just so much data out there and so many different entities have access to it that I just—you know, it is difficult to conceive exactly where you end all of this—for those of you, particularly Mr. McGuffey and Mr. Sanford, who are not banks at the time and not regulated at this time.

Mr. SANFORD. Our experience and our focus has obviously been on our own industry. And if we look at what California legislation—which I believe got all of this notification started—it is specifically an identity theft piece of legislation.

And clearly, if there is personal identifying information that is subject to a compromise—whether that is information that I might have in my business, or another organization, a government agency, an institution has—clearly where there is a risk of harm, I think you would want to say that notification should be made.

Now, when you have medical records, which is personally sensitive information, that there is no risk for identity theft, that may a different issue from a policy standpoint whether you are going to provide notice, where someone wants to know that their personal medical information.

But I think if you have financial information, credit information or personal identifying information that poses a risk for identity theft, I would cast a broader net.

Mr. CASTLE. I guess the problem comes in trying to write this and put it into legislative language.

Do you have any comments, Mr. McGuffey?

Mr. MCGUFFEY. Yes. I would concur that if it is personally identifiable information, Social Security numbers, driver's license numbers, that are full numbers, and an entity, whether it is public sector, academic, or even other businesses in the private sector, retail or otherwise, if they are handling that kind of information and allow that information to get into hands that are inappropriate, then that is where we ought to be evaluating legislation to make sure that there are proper controls in place.

As we have already stated here, a lot of the security under GLB does not extend there. We obviously, when using that data, have obligations under GLB for proper, permissible use of it. But the handling of that data by many organizations is no different from a threat standpoint, in my view.

Mr. CASTLE. Thank you.

Ms. Maloney is recognized for 5 minutes.

Mrs. MALONEY. First of all, I want to thank the Chairman and Ranking Member for calling this hearing. It appears we truly do have an epidemic of security breaches.

I just want to give one example: MSNBC reported that from mid-February through April, data breaches exposed over 2 million Americans to credit card fraud and identity theft, which is a huge exposure.

From your testimony, it is clear that it is a large range of entities, from banks to universities to retailers, and I would say a very wide range of consequences.

Mr. Bachus pointed out that many financial institutions are already covered under Gramm-Leach-Bliley and the FACT Act. But

I would like to ask the panelists if you could clarify further on Mr. Castle's question on how big should the covered universe be, and should the same standards apply?

For example, financial institutions have access to more sensitive data than other entities may have—and your comments on that and how do we define it, the extent of it.

I would also like to ask about the need for an objective bright-line standard for notification, particularly when there is personal identifiable financial information—and if you would like to comment on whether you think all entities should have a bright-line standard or only certain ones.

And I welcome anyone's comment.

Mr. MCGUFFEY. Well, as I think most of us have testified here and indeed my view is that I do not see a great deal of difference between an academic organization or a private sector organization when the information is the same. When you have a full Social Security number that is allowed to be accessed inappropriately, the impact, it seems to me, would be the same.

So I would support and our testimony is that it is not the organization; it is the information and then it is how or the danger that is caused as a result of that.

Mrs. MALONEY. Any other comments?

Mr. WARD. Yes, Representative, I would like to respond to your question.

There is a tremendous amount of information. Everybody knows that. And it is so extensive and there is so much of it that it needs to be properly disposed of.

For example, if you had come to work for me in my organization in your previous life, under our guidelines and under our certification process, I would have a human resources file on you that would have your drug test, would have your criminal background checks, would have all kinds of personal information.

And then at such time as you ran for Congress and were elected, I may not have a particular need for that file and it had outlived its usefulness, I could simply throw in the trash can, with no guidelines. And that information would be out for any Dumpster-diver to find. So it is a very broad issue.

We think that each company should have some type of employee or customer-consumer disclosure that outlines exactly what information it has and how it should be disposed of.

Mrs. MALONEY. Thank you.

I would like to hear the views of Ms. Desoer and Mr. Sanford on the need for a consistent standard of data protection.

Ms. DESOER. Yes. Being a financial services institution, we do have a consistent national standard in the Interagency Guidance and in all of the regulations that were referenced, and we believe that is appropriate.

I would like to reinforce that, again, I think the place that it should start is what personal information is being collected and being used as the criteria for who should be subject to some kind of a national standard.

Mrs. MALONEY. Mr. Sanford?

Mr. SANFORD. On data security provisions, what we think is workable, again, are the safeguards that are under GLBA.

And the reason why I think they are more workable than a specific standard is, I think when regulation attempts to prescribe for each and every business exactly how their security should be deployed, it does not take into account differences in technology, it does not take into account different applications and uses.

And the GLB safeguards put the burden on the corporation to continued to enhance the security of their business as new threats emerge. It is not a static set of standards, and instead it is a set of standards that you have to continually publish, upgrade and monitor to face new threats.

Mrs. MALONEY. My time is up. Thank you.

Mr. CASTLE. Thank you, Ms. Maloney.

I will yield myself 5 minutes.

Let me start with something that has been touched on. Actually, this is a useful hearing because we are really trying to develop legislation, and your input is very, very important to that.

And I think, Mr. Sanford, I will ask you the discussion, because you mentioned in one of your answers to one of the questions about the significance of security breaches.

And I think there are levels of breaches, obviously. I mean, I am not an expert on this. But clearly there are levels by numbers, there are levels by the extent of what is in the information that is breached and a whole variety of probably other things I have not even thought of.

But my question to you is: Do you believe that we should be trying to put in legislation the different level of breaches that would indeed trigger notice or whatever the remedies may be—as one part of the question.

And the other part of the question is: If not, who will do that? Should that be left up to the individual entities who are dealing with it, be it LexisNexis or Bank of America or anybody else?

Exactly how should that whole business of what triggers the various breaches and the measure of the breaches be handled?

Mr. SANFORD. Congressman, where I start my thinking on this is: What is the intent of providing a notice in the first place? So if I got a letter in the mail, like my sister did, from my company, what do I do with this? Why did I get this?

And the reason why she got that, along with the other people we sent notices to, is because we said there is some risk of harm and you need to take corrective measures. You need to look at your credit reports, you need to take advantage of these services, et cetera.

So when I think about what triggers, when you talk about a level of notice, to me it turns on whether or not there is a risk of harm—again, I am talking about identity theft-based legislation, not security-breach legislation; that is, to me, a different issue—is if there is a risk of identity theft because of a security breach in a business, where that information—financial information, credit information, personally identifying information—would enable that information in the wrong hands to put somebody at risk for identity theft or fraud associated with that, then I think there should be notification.

I think it should be national. If you think about the mobility of our society and how frequently people move, and you can see down

the road where we may have 5, 10, 15, 20, 25 different state standards coming out, and different triggers, different forms of notice, different remedies, and you get people moving around, my guess is we are going to confuse most Americans if they are getting these notices in the mail that tell them they need to take appropriate action.

Mr. CASTLE. Thank you.

Ms. Desoer, sort of a follow-up on that question, and instead of dealing with this issue and this problem of preparing legislation, we have heard from a number of financial institutions on how they believe notification should be structured when a breach is outside of their scope. Some want the opportunity to inform their customers while others believe it should be the responsibility of the breaching entity. What are your thoughts about this?

And I recognize the fact that this is extraordinarily expensive, and you sort of put your name on the line to a degree. So this to me is not a simple decision that you have to make or that we have to make in terms of preparing legislation.

Ms. DESOER. And I think that is key. It is not a simple situation, and it is a very dynamic environment in which we operate, in which lots of pieces of it are evolving.

So the approach that we have taken is really to evaluate each event separately and to work to get all of the facts together and the right people engaged, and then whether that is a merchants association, the financial services institution, whether it is directly between us and our direct customer, each one is slightly different and needs to be evaluated in a context, starting with, at the end of the day, our brand and what our customers look for in the brand is for Bank of America to be a trustworthy, secure financial services institution.

It is what is in the best interest of our customer, so that you have the spectrum of some of what you just heard, you do not overly confuse the customer, the ultimate consumer, and it is easy for them to know what it is is in their control and they can do to the other end of the spectrum where it is very specific and explicit and it is step one, two and three.

And so each one does need to be evaluated, and that is why we believe that the Interagency Guidance that financial services institutions do operate under, there is some wording in there that directs us to evaluation of event that could reasonably lead to the misuse of the information. And we think that is an important part of whatever we do.

Mr. CASTLE. Well, my time is up. But what you say makes it difficult for us, as you can imagine. Because if we legislate in this area—and I believe with of all of you, I think all of you are saying, and that is, we need to approach this in a national manner or we are going to have tremendous problems, State by State.

But in doing so, to draft the kind of language that will have applicability beyond financial institutions to other entities dealing with data as well, and to try to determine the manner of breach, the remedy of the breach, all these kinds of things, is going to be extremely difficult.

So I would just hope you would encourage everybody who is interested in this to get in touch with all of our offices and let us

know what your thoughts on it, because this is not going to be that easy to do.

I yield 5 minutes to Mr. Frank.

Mr. FRANK. Thank you, Mr. Chairman. I apologize for being in and out, but I had to go name a post office—an important part of our duty. Actually, this kind of an important one.

I want to first say that, with regard to Ms. Desoer, I thought the Bank of America's response was a very good one. And I think we are sometimes critical when institutions do not do what we think meets their responsibilities. In this case, Bank of America stepped up and did more than they were legally required to do. That is important.

I have to say to people in the business community in general, the financial institution, we are sometimes told two contradictory things: One is, "Don't legislate right up to the very edge. Leave us some discretion. Don't overdo the legislation. Put some general laws in there but trust us to be sensible."

But then we run into situations where something is not done that we think should have been done, or something is done that we thought should not have been done, we think it did not really fully treat the customers in the right way and we are told, "Well, we complied with the law."

In other words, sometimes we are told, "Don't push the law too far." But then, the kind of catch-22 is, people say, "Well, we did not have to."

And people should understand that, that if the institutions are going to be very literal and insisting that they will do what the law requires and nothing more, then they should not be surprised when the law may in fact go further than they want to do.

In this case, Bank of America reached out and did more than the law required, and I think that was very useful.

Another point, I notice there has been some reference to people saying, "Well, you do not want us to have to notify you every time there is a breach because we will be flooding people with paper."

I said that before, I must tell you, particularly to my friends in the financial community, you are not credible when you say you do not want to send us unsolicited mail. No one sends me more unsolicited mail. I have constituents who do not write me as often as you do, and they have a better claim on me.

So that, I have to say, when people give me a reason that I do not believe, then I have to wonder what the real reason is. And I do not think it is an aversion to sending out unsolicited mail that is involved.

So if there is some problem that is triggered by your having to notify every time there is a breach—and I have to say, I do not know what standard you could come up with that would say, "We are only going to tell you about a breach if we think it is likely to cause a problem." We are not going to know in all the cases what happened.

I suppose if it was purely accidental, you might say there was no likelihood, but we do not know what will show up.

The other—and I was very pleased Mr. Foley testified. In fact, I was hoping that we could get someone to ask him to do this.

I must say that when we dealt with the extension of credit, I was disappointed with the response from the retail industry. At the time what we were talking about was how do you resolve a dispute if you are told by the credit-rating agency, "Well, you did not pay this bill," and you say, "Hey, I never bought that thing. That was not me," or, "Yeah, I bought it and I returned it, it was defective," or, "I paid for it."

The retail industry was very resistant to having any obligation to go back and check as to whether or not there was substantive mistake. Their position was that the most they should have to do would be to check the paperwork.

And in fact, we had studies that showed they did about, I do not know, 40 of those an hour, that there was no way the consumer could get some kind of independent investigation. Now, we moved a little bit towards that.

But now, again, I find the retail industry in some ways being resistant. I am told that they said, by credit unions in Massachusetts, that when BJ's, I guess it was, had the—what is BJ's? I do not want to—albeit, I am immune from liable suits, I do not want to abuse the privilege.

But BJ's was responsible for breaching security of data, and the institutions that issued the cards, as Mr. Foley has indicated, had to tell the cardholder, "Well, your data has been breached, but I do not know who did it and I cannot tell you who did it." My sense is that most of them did not believe you. They thought you did know and did not want to tell them.

That just seems to me unacceptable, especially since the general rule in our legal system is: You ought to put the most responsibility on the people who have the ability to prevent the abuse.

Now, the people who have the best chance to prevent the abuse of data are the people who are handling the data. And it just seems to me an elementary example of basic logic: Whoever was the one entity that was responsible for the breach ought to have to be identified.

That in and of itself, it would seem to me, if we just did that legislatively we would be doing a great deal I believe to reduce breaches. We would then greatly ratchet up the importance of reducing breaches in people's minds.

So I know what Mr. Foley thinks. I wonder if any of the others have any comment on requiring, whether it is the retailer or anybody else, to the extent that we know who is responsible making that public.

Let's start with Ms. Desoer.

Ms. DESOER. I do not have any issue with that. I think some of the issues between the retailer or the merchant and the financial services institution is confidentiality of a client relationship and the priority that that takes in terms——

Mr. FRANK. What kind of—I mean, what, the people did not know—there is no—what we are here talking about is that somebody has a credit card that you issued and they used it at a particular merchant. There is no confidentiality there.

Ms. DESOER. No, but if retailer X, for example, has a banking relationship with Bank of America, our relationship with them does

not enable us to talk publicly that we have a relationship with them.

Mr. FRANK. Well, then we ought to change that law.

In other words, if you are saying that because I got an account in your bank, if I screw up in another way, the bank cannot identify me. That just seems to me unnecessary.

Ms. DESOER. No, that—and that is not what I am implying. It is, again, going back to the ultimate consumer who is, in this case, our credit card customer and our communication to them. I hear you relative——

Mr. FRANK. Yes, what I am saying is——

Ms. DESOER.——excusing as to who is at fault——

Mr. FRANK. You do not have to do—if the retailer messed up on the data, that does not mean you give a list of all the retailers' confidential financial information, but identifying that that is where the breach came. I do not see how that is a problem with your confidentiality.

Ms. DESOER. I particularly aligned with what you said, which is the responsibility of whomever is collecting and managing that information should be the one accountable.

Mr. FRANK. If others want to do a quickie, my time is up, I will just listen.

Mr. MCGUFFEY. We at ChoicePoint agree that ensuring that the burden of notice follows responsibility for breach is appropriate.

Mr. FRANK. Thank you.

Mr. SANFORD. Congressman, we are not a financial institution, we do not have retail, but in our security breaches, the breaches occurred in our customer environments where their password and I.D.s were compromised through a variety of methods, and we saw it as our responsibility as the party who maintained the databases where the breaches occurred to make the notice.

Mr. FRANK. Mr. Ward?

Mr. WARD. I am not sure that I have a particular comment in respect to that question.

Mr. FRANK. Well, if you are not sure, nobody else could be either.

[Laughter.]

So I guess that is one uncertainty that will go unresolved.

Mr. WARD. We are not in the retailing business and we do not deal with any particular dynamics.

Mr. FRANK. Okay, thank you, then, that is very responsive.

Mr. PRICE. [Presiding.] Thank you, Mr. Frank.

Mr. Castle and Mr. Bachus, we have the FDIC bill on the floor currently, and so they apologize for not being able to remain for this portion of the hearing.

Mr. McHenry from North Carolina is recognized.

Mr. MCHENRY. Thank you, Mr. Chairman. It is pretty nice to hear a freshman as a chairman of such a big committee.

Thank you all for testifying here today.

And my question is, just generally speaking, really to ChoicePoint and Bank of America mainly: Is there currently not a marketplace incentive for data security? Do you not see an economic incentive in terms of your communication to the customer?

I live in the suburbs of Charlotte, and really just right close to your headquarters of Bank of America, and I certainly understand

the advertising that you currently have about the secure network that you do have in place, the fact that you do not have errors when it comes to check processing, things of that sort. And there is an economic incentive I see to that marketplace on security. I was wondering if you all could address that.

Ms. DESOER. Yes. As I said in my testimony, what customers come to us for is trust and security, and we take that extremely seriously. And the stewardship of customer information and their privacy and all that goes along with it is, at the end of the day, what our brand stands for.

So it always starts with what is in that customer's best interest. We firmly believe that our ability to earn that trust and to demonstrate our ability to manage that trust over the lifetime of a relationship is what differentiates us in the competitive marketplace, yes.

Mr. FOLEY. I would say that in looking at the issue to remember that the security is only going to be good as the weakest link in the fence. So as we are looking at these issues, there is no current economic benefit to many of the parties that touch that data, to protect that data.

Mr. MCHENRY. Do you want to further elaborate?

Mr. FOLEY. In particular, my own experience, when we are talking about the large-card associations, mostly Visa and MasterCards, regulations on the merchant versus the card-issuer, between Gramm-Leach-Bliley and all the other regulations that the issuer has on them, no matter how much they protect them, if the same standard is not dealt with in particular merchant, then whatever effort and resources the issuer is putting behind the security is meaningless, because there is no incentive for that merchant to do anything other than to get that payment through their system as quickly as they possibly can.

Mr. MCHENRY. Are you not fearful of lawsuits and repercussions because of lax security?

Mr. FOLEY. Well, that is right now what the remedy is. And as I had said in my testimony, in the case of BJ's Wholesale Club, there were 40,000 cards that were compromised within about a 2-week period. Credit unions have brought suit and individual banks in Massachusetts have brought suit. And right now that is the only remedy.

Mr. MCHENRY. Really, the question goes to the heart of, is there not an incentive in the marketplace to do this without governmental intervention?

Mr. FOLEY. If the lawsuit comes out favorably for us, yes.

Mr. MCHENRY. All right. Well, thank you for your testimony.

Mr. PRICE. Thank you.

It is my pleasure to recognize the gentleman from Georgia, Mr. Scott.

Mr. SCOTT. Thank you very much.

Mr. McGuffey, let me start with you, if I may.

Going back to this winter, February, when the news came out about the identity thefts, ChoicePoint was immediately hit with an order by our insurance commissioner to give you 90 days to put some things in motion to correct the situation. I would like to ask you just a line of questioning on how you have fared with that.

One of those points was that you had to provide immediate notification. Can you tell us how well you have done that so far?

Mr. MCGUFFEY. Yes, Congressman, we have provided notice. And indeed, we are I believe in process of and if not having already made notice to California at the time when that request had been made.

Mr. SCOTT. So that point has been satisfied to the satisfaction of the insurance commissioner in Georgia.

Mr. MCGUFFEY. I believe so.

Mr. SCOTT. That is very important, because there is a part of that he said if not in 90 days you will be barred from doing any business in Georgia with insurance companies.

The second point was that you had to establish a rapid response system. Have you done that?

Mr. MCGUFFEY. I believe that we have formed a team to be able to respond to that. The details of that, today, I am not prepared to speak to, but I would be more than happy to provide it to you and your office.

Mr. SCOTT. Okay. And the third item that he said you had to do within 90 days was to perform a system-wide audit with an independent security firm. Has that been put into place?

Mr. MCGUFFEY. We have retained the services of an independent firm. I am not sure as of this date as to whether it has been completed or not. But if it has not been completed, we are in process to be able to achieve that objective.

Mr. SCOTT. Has the insurance commissioner been made aware of the level of progress that you have made, that you have expressed here, to this point?

Mr. MCGUFFEY. I am not aware of the details of what we communicated back to the insurance commissioner at this date.

Mr. SCOTT. Do you have concerns that you may not be able to make this 90-day period? This occurred in February. It is now May. Time is running out. Do you feel any concern that you might not be able to make the 90-day deadline?

Mr. MCGUFFEY. I have not heard of a concern that we would not be able to meet those requirements.

Mr. SCOTT. Let me ask you another question. Let's get our hands around this issue. There has been some discrepancy pointed out as to the extent of this problem.

By last estimates and your most accurate accounting, I believe it has been 145,000 records that were stolen. Has that changed any, particularly in view of the light of the discrepancy that was brought to our attention from California by Detective Decker, that you had estimated at 17,000, and he said it was more like 4 million. That is a huge difference.

Mr. MCGUFFEY. Yes, Congressman. I think the comments that were in the Wall Street Journal yesterday—which we tried to get a good insight on, having seen that yesterday for the first time—those comments by Detective Decker were made in the very early stages of his investigation. In fact, as I understand it, from what I have been told, those comments were made at the arraignment of the individual who was arrested.

At that time we had not completed our investigation and rebuilt all of the searches that had been run—there were over 17,000

searches that had been run on our systems—nor had the sheriff's department completed their investigation.

Now that we have progressed in the investigation to this date, we have been informed by Detective Decker that he is in agreement with those numbers and believes that our notice was appropriate and consistent with his review of the records.

Mr. SCOTT. All right. Let me ask you one other issue before my time runs out, because one of the very, very important areas that this committee deals with is in the financing of terrorism.

ChoicePoint has developed an excellent reputation of assisting in that fight against terrorism. Would you care to share with this committee some examples of the effectiveness of ChoicePoint in our war against terrorism?

Mr. MCGUFFEY. Thank you, Congressman.

We are obviously very proud of our opportunity to work with Homeland Security and other law enforcement agencies to pursue the—of making sure that our country is safe.

We have products and services out of our—on data services that are in Homeland Security that enable our law enforcement to investigate rings and investigate terrorists. We have examples there, although oftentimes since I am not—have a security clearance, I will not hear about them all.

But that is one example where we are delivering a technology into Homeland Security. We have on a daily basis the various, different agencies—FBI as well as sub-agencies of FBI—use our services in order to investigate leads that they may get.

We have built specialized systems for them at their request, to their requirements, in order to support those organizations, and we are proud to be able to do that.

Mr. SCOTT. Thank you.

Thank you very much, Chairman.

Mr. PRICE. The gentleman's time has expired.

The gentleman from New Mexico, Mr. Pearce, is recognized.

Mr. PEARCE. Thank you, Mr. Chairman.

Ms. Desoer, is there any resolution to the case where you lost the five tapes?

Ms. DESOER. No, there is no resolution. The investigation is still ongoing. We have continuously monitored those 1.2 million customer accounts, and there is no evidence that the information——

Mr. PEARCE. Have you had any other losses of significant size of identity theft, just people getting information?

Ms. DESOER.——lost tapes or that sort of thing? No. I mean, the retailer situations, the merchant situations that have been referenced, we have a significant cardholder customer base. So——

Mr. PEARCE. Mr. Sanford, has LexisNexis ever experienced any losses of information? On page 2, you describe the enormity of the situation: 9.3 million cases. Have you had any losses of information through your system?

Mr. SANFORD. In my testimony I indicated what we discovered in the investigation that we did.

Mr. PEARCE. And how easy is it to get convictions on any of these things? How easy is it to track down the people who are doing it and then to get convictions?

Mr. SANFORD. Well, I have been working with the U.S. Secret Service since the end of February, and we get regular briefings. And it is extraordinarily difficult, with their resources, to gather sufficient evidence for the warrants and the manpower to then chase down.

It is a whole level of sophistication in the underground economy that is trafficking in this information. And I frankly believe that we are out-manned in law enforcement. I think it is very, very difficult. They have had some successes that have been very public.

But I think until the penalties on identity theft are much bigger than the value of the theft, I think that you are going to continue to see rampant identity theft—the old-fashioned way too. Most of it is still your friends and your family and your neighbors committing this.

Mr. PEARCE. How easy would it be to close the opportunity, the window of opportunity, between the time something happens and the time we actually then get it closed down—Ms. Desoer, if you could address that?

Ms. DESOER. Yes. Immediately upon discovery, we start monitoring accounts. And so while an investigation is ongoing, we will know if there is unusual activity. And customer by customer, we can handle that immediately to either reassure a customer's card or take whatever action is required to protect them.

Mr. PEARCE. But the losses are still enormous, I mean, billions even in that narrow window. Is it possible to close the window even tighter?

Ms. DESOER. That is what we are working very hard to be able to do, to provide that protection of the customer and then also protect the financial loss.

Mr. PEARCE. Who determines when a customer should be notified and who has the authority to do that?

Ms. DESOER. Within Bank of America, we are subject to the Interagency Guidance and the federal regulations that guidance talks to when there is information that could reasonably lead to the misuse of the information.

We have the equivalent of a rapid response team that evaluates each situation and makes the judgment call, taking into consideration the best interest of our customers.

Mr. PEARCE. The recent case in my hometown, someone's identity was stolen by a group of people in prison. They were simply sitting there using their time either constructively or destructively, depending on which point of view. And literally, the law enforcement officer said that no action was available, they are already in jail, they are already criminals.

And so I suspect if you have recommendations on ways that we can change the laws, that we would be open to that.

Mr. McGuffey, do you think you are going to get any resolution? Do you think you will get a conviction out of any of the things that you all face?

Mr. MCGUFFEY. Fortunately, we have had two convictions. Unfortunately, I believe the first conviction was only, like, 16 or 18 months in jail, which we wished were longer. The second one I think was a five-and-a-half-year sentence.

Mr. PEARCE. How easy is it—I think I would go back to you, Ms. Desoer—how easy is it when someone actually comes up with information, they get a card number, a Social Security number, how easy is it for them to use that information, like Mr. Foley experienced? Is it easy: Or is somewhat difficult?

Ms. DESOER. I think each circumstance is very different, depending on what the sophistication level is of the individual, whether they are operating independently or part of a group. It varies across the board.

Unfortunately, as someone mentioned, it depends on where there are weaknesses anywhere in the system that impact—they are not as strong potentially as they should be relative to authentication or identification of a customer where they could sort of infiltrate and as a result get access to the funds in the account or something like that.

So it can be quite easy if there are weaknesses in the system and someone is sophisticated about knowing how to identify those weaknesses and penetrate them.

Mr. PEARCE. Mr. Foley, my time is expired, but you are more than welcome to answer.

Mr. FOLEY. I was just going to say that on the mag stripe is now a three-digit algorithm that relates to the PIN number on the front of the card, if that algorithm is captured, that card can be remanufactured and used regardless of the name or any other information associated with that account.

Mr. PEARCE. Well, I thank you all for your leadership in this very difficult area. I appreciate your testimony today.

Mr. Chairman, I yield back.

Mr. PRICE. Thank you, Mr. Pearce. The gentleman's time has expired.

The gentleman from Kansas, Mr. Moore, is recognized for 5 minutes.

Mr. MOORE OF KANSAS. Thank you, Mr. Chairman.

To all of the members of the panel, are there other instances of personally identifiable information which have been compromised—I mean, lost—by any of your organizations that have not been identified in your testimony here this morning or in your either written or oral testimony that you have not disclosed?

I would like an answer, yes or no, from each of the panelists, if you would, please.

Mr. WARD. No, sir, my company has not experienced——

Mr. MOORE OF KANSAS. Mr. Ward—I am sorry, go ahead.

Mr. WARD. No, sir, my company has not experienced any losses of that nature. In fact, our organization, the National Association of Information Destruction, we have about 650 members in that organization, and we are not aware of any kind of willful loss or anything of that type.

Mr. MOORE OF KANSAS. Thank you, sir.

Mr. Sanford?

Mr. SANFORD. We have disclosed in our testimony our breaches that related to the risk that we thought——

Mr. MOORE OF KANSAS. None other than what you have disclosed.

Mr. SANFORD. Well, you have situations where an employee of the company might leave a company and continue to do a search the next day. We did not make notice on those. As I indicated, we made notice where we thought there was any evidence of any possible risk of identity theft.

Mr. MOORE OF KANSAS. Thank you.

Mr. McGuffey?

Mr. MCGUFFEY. We have previously testified in front of this committee, as well as others, that the Social Security numbers and driver's license numbers were the personally identifiable information that was disclosed.

Mr. MOORE OF KANSAS. Thank you.

Mr. Foley?

Mr. FOLEY. My company has not had a breach. But as a matter of course, on a routine basis, this is happening every day, not only these large-scale breaches that you are hearing about but identity theft is happening on a small scale simultaneously to this.

Mr. MOORE OF KANSAS. Ms. Desoer?

Ms. DESOER. We have had no other issues related to lost tapes. We have had instances in the past where there have been similar processes followed to identify losses of information in addition to those that were referenced in my testimony, yes.

Mr. MOORE OF KANSAS. Thank you.

To the panelists: Is there a state model?

Some of you have talked about "we support"—in fact, I am looking at Mr. McGuffey's written testimony: "We support a preemptive national law that would provide for notification to consumers and to a single law enforcement point of contact when personally identifiable information has fallen into inappropriate hands."

Is there a state model, a law, that you would recommend to this committee that we look at and maybe follow in terms of drafting legislation to protect consumers in this area?

Mr. McGuffey?

Mr. MCGUFFEY. We modeled our nationwide notice after the California law. We think that there are some provisions in that law, however, that need to be reviewed and discussed and debated. But we modeled ours after California, which I believe was the first state to have such regulations.

Mr. MOORE OF KANSAS. Mr. Foley, did you start to reach for your button?

Mr. FOLEY. I did. I was going to say, also, as I agree with Mr. McGuffey around the California law with some additional definitions and provisions.

The other advantage to that legislation I personally feel is that in terms of media accounts delineating the scope of this issue, I believe it was really the California law's requirement for disclosure that has helped flush this to light.

Mr. MOORE OF KANSAS. Anybody else on the panel have comments there? Mr. Ward?

Mr. WARD. Yes, sir. Actually, this committee, through the FACT Act, has drafted some legislation with regard to the disposal rules. They could serve as a model for any other legislation.

The FACT Act drew a line around consumer report information, and if those lines could be removed where it could stretch across

all businesses, that would serve as what we were trying to accomplish.

Chairman Majoras at FTC has also discussed this——

Mr. MOORE OF KANSAS. Thank you.

Mr. Sanford?

Mr. SANFORD. Congressman, I applaud the intent, the legislative intent, of the California statute. But I think the drafting really does need quite a bit of work in terms of the triggering events and the form of the notice.

The consumer division in California came behind that legislation and provided some very, very helpful guidance, but it is not binding, and it is not the law in California.

So I would encourage the committee to take a look at both of those.

Mr. MOORE OF KANSAS. When you mention triggering events, do you have any specific recommendations with regard to what triggering events should institute a procedure here?

Mr. SANFORD. Well, I think, again, the California law does provide some examples of very specific things that would be a triggering event, if you had the loss of the physical custody of data on, for example, a personal computer—well, excuse me, I apologize. That is in the consumer division guidance where they begin to really give examples.

But I think that the risk of being very specific is that you will fail to then consider a breach that does not specifically fit within one of those guidelines when a reasonable person could conclude that a significant risk of harm still existed to individuals and that notice should be made.

So I think this reasonable standard and then specific examples that say this per se requires notice of loss of physical custody of data on a P.C. or on a tape—that should trigger.

Mr. MOORE OF KANSAS. I see I am out of time.

Thank you, Mr. Chairman.

Mr. PRICE. Thank you.

The gentlelady from Florida, Ms. Brown-Waite, is recognized for 5 minutes.

Ms. BROWN-WAITE. Thank you, Mr. Chairman.

I have a bit of laryngitis, so I hope you all can hear me. As some say, this is a husband's prayers answered. I am not sure.

Some members, I have been told, are considering legislation that would make it illegal to sell an individual's Social Security number without permission. What effect do you think that would have on the American economy and your business in particular?

Do you want to start down there?

Mr. WARD. Yes, ma'am. Actually, a Social Security number cannot be sold, but it could actually be thrown away. You can dispose of it right now in the Dumpster, and that information is not regulated once it goes into the Dumpster.

With the proper disposal rules, that would certainly go a long way toward preventing some of the identity theft that is occurring through that route.

Mr. SANFORD. We use Social Security numbers in both public records and nonpublic-record information to link disparate pieces of data. I mean, there are 20,000 John Smiths or John Williams out

there. If you were to take away the unique identifier of an SSN, then the ability to match disparate pieces of data would defeat the tools that financial institutions, law enforcement, Homeland Security and other organizations use to make sure that they have the proper person identified and verified that they are doing business with.

And in fact, in my opinion, you will then enable greater identity theft, because you will take the tools out of the hands of those institutions which are catching a lot of the fraud that is happening.

Mr. MCGUFFEY. Yes, we would concur that the use of Social Security numbers for fraud and for proper identification of individuals in validation of individuals who are seeking access to either a system or other benefit that they may have need to.

We also have made some voluntary changes to our business and are restricting, in certain markets under certain circumstances, the distribution of full Social Security numbers. But we still use Social Security numbers in order for matching to make sure that we are associating the proper records together.

Mr. FOLEY. Financial institutions have been protecting Social Security numbers for some time now. I think that the only application that I can think of where it is most prominent is in IRS reporting data.

Ms. DESOER. I would concur with that and also what the other gentlemen have said relative to ways of matching customers for purposes of determining credit qualifications and that sort of thing is highly dependent in this country on a Social Security number.

Ms. BROWN-WAITE. Well, with a name like Virginia Brown, I can just tell you that there are many, many Virginia Browns out there, and I can relate to that.

Ms. Desoer, just a quick question: A constituent of mine who used to use the online banking offered by, in this case it happened to be your bank, but any of the banks that offer online—or any of the financial institutions, this certainly would apply. His comment was that with wireless and with spyware, he no longer is comfortable using the online bill-paying service.

What response would you have to that individual who felt that his identity and information about his bank account would be too easily available?

Ms. DESOER. I would need to understand the specific circumstances of how he was accessing online banking. But we do a tremendous amount, obviously, to protect the flow of customer information from just about any device to our online banking application. And it is a constantly evolving technology.

We also provide advice and counsel to our customers about what type of protection they should employ to ensure that, on the receiving end where they are, at work or at home, that they are adequately secured as well.

But I would be happy to get a name from you and follow up with that customer in particular.

Ms. BROWN-WAITE. Just one follow-up question: Do you advise people on the use of wireless?

Ms. DESOER. I need to follow up with you on that question. We do make suggestions about what the most secure ways are, but rel-

ative to wireless and specifically in what we are telling customers today, I would need to follow up with you. Thank you.

Mr. PRICE. The gentlelady yields back.

The gentlelady from Oregon, Ms. Hooley, is recognized for 5 minutes.

Ms. HOOLEY. Thank you.

I would like to ask all of you, the question is—one of the things you can do is voluntarily provide access to credit-monitoring services. How many of you have done that and for how long? And do you do it for free?

Ms. DESOER. At Bank of America, in our particular case with the lost tapes, we have offered the credit-monitoring services, and we have offered them for I believe it is up to a year—it is for a full year.

Ms. HOOLEY. Is that free?

Ms. DESOER. It is free of charge. It is at Bank of America's expense, yes.

Mr. FOLEY. For most of the smaller financial institutions in the country, they need to rely upon Equifax and the large credit bureaus and the free credit reports that each customer can get on their own. They do not have the resources to provide that for them.

Mr. MCGUFFEY. In ChoicePoint situations where—all of the cases that we provided notice, we provided a 1-year monitoring program at ChoicePoint's cost.

Mr. SANFORD. We provided all of the services—the tri-credit bureau, the monitoring, the counselors, the fraud insurance—all of that at our cost.

Ms. HOOLEY. For how long?

Mr. SANFORD. The credit monitoring is for 1 year, and then if somebody is a victim of identity theft, we just evaluate them on a case-by-case basis.

Mr. WARD. In our particular industry, we do not have any access to credit information, but we do have some exposures and liabilities for the loss if we were to lose something. Everybody in our trade association is required to carry certain amounts of insurance and subject it to all types of background checks.

Ms. HOOLEY. I have worked for a long time with identity theft, and one of the constants I hear at lots of my meetings is a need for a second-factor authentication. What do you think about that? Is there a need for a second piece to make sure the people are who they say they are?

Mr. SANFORD. I will go ahead and start.

I know some of the European banks, the financial institutions, do use double factor, two-factor authentications. Some use even a third layer.

That is something we are looking at. There are tokens and smart cards available in the market today. They are not inexpensive.

But we are evaluating that ourselves right now to see whether or not we could deploy two-factor authentication for certain of the accounts—because, remember, all of our accounts do not access personally sensitive information—whether we would be able to use two-factor authentication and would the market accept that.

One of the members asked earlier: Is not there a competitive advantage or an economic interest in doing that in being the security company.

The reality is, is that to the extent that customers deem it to be an inconvenience and they have 15 other organizations they can get the same data from and not manage 20,000 tokens for their users, we would probably be put at a significant disadvantage.

So I am trying to figure out how we do this. I am not suggesting that we should legislate it. But what I am saying is, are there disincentives to us doing it and putting ourselves out of businesses.

ChoicePoint and LexisNexis mask Social Security numbers and driver's license-number data. Most of our competitors do not. And so people who want that data just go to somebody else. We do that voluntarily as a matter of policy.

Ms. HOOLEY. I mean, one of the things, identity theft is costing all of us a ton of money, whether you have been an actual victim or not. I mean, all of us end up paying for that theft that occurs.

And how do we—I mean, what do we look at to help stop identity theft?

And, again, it may be for someone else—and I would like to hear from Bank of America, if you are looking at a second piece of authentication.

Ms. DESOER. Yes. We are constantly evaluating, ensuring that our authentication and identification processes are as secure as they could be. We are testing in the online-banking environment a second factor, and we have it operational in our card environment today.

Ms. HOOLEY. Anyone else want to comment on that?

Mr. MCGUFFEY. We are evaluating the tokens as well, and I concur with Mr. Sanford's comments.

In addition we have offered some products and services that are called "smart questions," which enable institutions or customers of ours to be able to not only just validate certain pieces of information, such as the use of a name and a Social or something of that nature, but also to go to a second step where random questions about one's particular circumstance have to be answered in order to validate that it is who they say they are.

Mr. SANFORD. The question that we wrestle with as we have dealt with these security breaches is: Can we as a society—and I am not talking about just LexisNexis; I am talking about retail, financial institutions, data companies—can you stop the theft of data? How sophisticated is the technology?

And I do not mean to downplay the importance of us getting our security enhanced and being responsible, but if we think about this more holistically and we recognize the level of sophistication of technology and the criminal element, part of the solution to stop the fraud when someone gets that data is to begin to use stronger authentication before you issue credit cards, before you open bank accounts, before you do online transactions.

And it is not just my company. There are many companies that provide these services. And there is significant evidence that when those kinds of products are used, you can defeat a significant amount of the fraud associated with identity theft. You do not stop

the data from getting in the wrong person's hands, but you can then not enable them to profit by it.

Ms. HOOLEY. To use it, okay.

Mr. PRICE. The gentlelady's time——

Ms. HOOLEY. Thank you.

Mr. PRICE. Thank you. I will recognize myself for a period of 5 minutes.

I want to thank the members of the panel and commend you for the work that you do.

Also, since there is a great interest and many questions, so I would ask unanimous consent to allow members of the committee 14 days to submit questions for the record following testimony today—without objection.

There is a bit of a somber tone here, and I want to hopefully lift it up a little bit and congratulate each and every one of you for the work that you do. There are lot of bad guys out there. And you all I know are working hard to make it so that bad guys are not getting the information that they want to get.

Just to bring some light to that, I want to commend one of the corporate citizens in my district, ChoicePoint, and just highlight a couple of the items that were pointed out in Mr. McGuffey's testimony.

I think it is important to recognize that when ChoicePoint had the infraction and the breach that occurred that they voluntarily acted, that they were the ones that told law enforcement and that many changes were made, including a voluntary nationwide notification, dedicated call centers and a Web site, the free three-bureau credit reports and the 1 year of credit monitoring—all at ChoicePoint's cost.

I also want to point out—I know that all of you are assisting many authorities in stopping bad things from happening. And a number of the things that ChoicePoint has done is the Project Falcon that assisted in catching 10,000 criminals, including individuals convicted of murder; the I.D. of over 11,000 undisclosed felons and stopping nearly 1,100 individuals—or finding 1,100 individuals who were convicted for crimes against children. The Lord knows what kind of assistance that could have been in terms of helping citizens across our nation.

I also sense that there is a great enthusiasm among the committee for a new law, and that should be greeted with I think a sense of comfort on the one hand and a sense of trepidation on the other. We get a knee-jerk reaction when we identify a problem that there ought to be a new law.

So the law of unintended consequences is what I have a fear about. As a physician I know that the HIPAA regulations, the privacy regulations in HIPAA now make it so that your medical information and my medical information are now less private than they ever were, because what you do when you go into a physician's office is now sign away every right to privacy that you ever had.

So I would like to ask each of you if you have any thoughts about how far is too far as we go through this phase of attempting to write something that will help individuals in their identity-theft problems.

But how far is too far for Congress to go, Ms. Desoer?

Ms. DESOER. In the financial services world, we do have the recent Interagency Guidance, which I believe is a good model, certainly one that is operational today for us, and I would give that some time in the financial services industry to mature so we can get learning that could help perhaps us to changes that be made. But I would ask that that be looked at as one possible solution from a regulatory specific, or a legislative perspective.

Mr. PRICE. Thank you.

Mr. FOLEY. I echo Congressman Frank's concern around notification and how efficacious it is. What we also find is, even if we are doing notification today for a breach, that that account is not actually—money is not stolen for 6 months, 9 months down the road.

So I am concerned about the constraints and timing of the notification.

Mr. MCGUFFEY. I believe that a couple of the comments by Congressman Frank are also worth emphasizing, both ensuring the burden of notice following responsibility for breach, being one.

Number two, we also think that there is an issue that could be a negative consequence, and this is desensitizing such notices.

So having some sort of clearing house that would enable a notice to be made only one time, as opposed to multiple times, in the event that there are rings of I.D. thefts, individuals out there that they may access more than one company or get access to data in multiple instances about the same person, that notices not be given more than one time.

Additionally, I think the final comment I would make is with regard to the use of Social Security numbers is critical for matching purposes to make sure that we do not have false positives and to make sure that we are able to support the appropriate transactions in business.

Mr. PRICE. Mr. Sanford?

Mr. SANFORD. We are not suggesting that FCRA or FACT Act be reopened. We are not suggesting that GLBA be reopened.

What we are saying is, we are facing probably a gauntlet of state notice bills. I think there are something like 70 or 75 bills that have been introduced in states on either security standards or on consumer notice. And if we are going to have that kind of patchwork of legislation, that is where we would support it more of a federal approach with preemption that provided a standard.

Someone said to me, "Well, you just want to avoid the cost of having to comply with 20 or 15 different states." And I said, yes, it is going to cost me, but at the same time, I am not sure that the consumers who are going to get all these different forms of notices as they move around are actually going to understand, because each state is going to do it a little bit differently.

So if we are going to have legislation on notice, then we would think that a federal preemption would be appropriate.

Mr. PRICE. Thank you.

Mr. Ward, any quick comments?

Mr. WARD. Yes, sir, thank you.

We are all recognizing that the identity theft laws that are already on the books are really good laws. We are not suggesting in any way that any of those laws be rewritten or reopened.

What we would suggest is that perhaps FACT Act, which is a great law and has excellent disposal laws, allow those to be broadened to cover more industries, cover all businesses.

In addition to that type of FACT Act guideline, our recommendation would be to have a company disclosure in any type of agreement stating what the company's responsibilities are and what the company's method for disposal of all records would be, so that anybody would see and understand what that procedure is.

And then the last step would be to, under the sort of the guidelines of perhaps Sarbanes-Oxley-type laws, where the senior management has some accountability for setting up those procedures and has some responsibility to see that those disposal procedures are fulfilled.

Mr. PRICE. Thank you.

My time has expired. And I will have some other questions that I look forward to submitting to you.

The gentlelady from New York, Ms. McCarthy, is recognized for 5 minutes.

Mrs. MCCARTHY. Thank you, Mr. Chairman, I appreciate it.

I have to tell you, Mr. Ward, before I was appointed to this committee, my son gave me a shredder. And I said, "What do I need this for?" Since I have been on this committee, I understand why I need it. It does take a little extra time, but everything goes through the shredder now.

Mr. Sanford and Mr. Foley, both of you have had incidences where you personally have had identity fraud, and your sister has had identity fraud.

I was just curious: With your sister, on the notification that she got, was it easy enough for her to follow the instructions for what she needed to do? Or did she come to you to ask how to do it?

Mr. SANFORD. No, she actually called to give me a hard time because she wanted to know why I did not personally sign the letter. It is a serious matter. I mean, we sent this out to some 300,000 people.

Very simple: It provides toll-free numbers, it names the companies, it talks about the steps that you go through.

Again, whether she is the victim of identity fraud, we do not know. Some people think if someone has potentially gained access to data then you are a victim of identity theft or fraud. She has not suffered any financial harm. She has not detected any problem. She is taking advantage of the credit services.

I told her to take the letter seriously and to take advantage of the services.

Mrs. MCCARTHY. No, I am just curious, because, like everyone else, we get a lot of mail. Is there anything on the front envelope to notify the client that this is something they should not just toss but open it up, because a lot of people do just toss things without looking to see what is inside.

Mr. SANFORD. We mailed 30,000 notices. One of the first things we did when we discovered these breaches in this business, we acquired, was we contacted the State attorney generals' offices in all 50 states and the District of Columbia and Puerto Rico and said, "Here is what we intend to do. We are going to make notice nationally. Here is how we are going to do it."

We talked to the Federal Trade Commission. We followed some of the California guidance.

After we did the first round of mailing—we had this ongoing investigation looking back at the records of this company—some of the attorney generals said to us, "Well, you know, maybe some people just thought it was marketing and they threw it in the trash can." So we said, "What would you like us to do?" And they said, "Well, would you put stamps on the letters instead of using machine postage. Would you put something conspicuous in your return address area that tells them this is important information?"

So we did. We remailed all the letters, again, to the first 30,000, and we used that approach for the second group that we mailed to.

Mrs. MCCARTHY. And was the response better?

Mr. SANFORD. The response rate is marginally higher. It is not significantly higher.

Mrs. MCCARTHY. What about, like, with the IRS "tax information enclosed." Everybody always opens that. How about "credit information"?

Mr. SANFORD. Well, I think this is where some of the panelists and some of the members have talked about. If you had a national clearing house where if letters came through that, perhaps people would recognize that, "Oh, this is an important piece of information."

I am sure there is a way to make the envelope even more conspicuous so that people will recognize there is information.

At the same time, I have some attorney generals telling me if I make it too conspicuous—since a lot of identity theft happens by people stealing other people's mail—I am going to turn around and give the bad guys information that is going to allow them to gain access again to this person's account. Because they will call up, they will purport to be who they are, they will get free credit reports on this person. It is a balancing act.

Mrs. MCCARTHY. Mr. Foley, how long did it take for you to clear up the information that was stolen from you?

Mr. FOLEY. That process was pretty readily done. Within Regulation E there is a 10-day window that the financial institution has got to be able to make you whole in your particular account.

In my case, the notification letter was received probably I want to say 6 weeks prior to my account being cleaned out. And the notification letter—I do not have it with me, but I kept—did not give me any particular call to action in terms of what I needed to do. It opened up a case number and said, "Just watch your account."

In my own case, as I literally sat in my office looking online at my account, I was watching myself buy a handbag in California and some very nice women's shoes, and my account was cleaned out probably about 6 weeks later.

I suspect, in terms of the notification itself, that it would not compel someone necessarily to take any action in particular.

As a credit union with a very close relationship with our members, typically what happen is if we have enough suspicion that the account may be breached, we just automatically do a reissue to protect somebody in that case.

My account was with a large commercial bank. And when I did contact them, they were very solicitous in terms of realizing that

the transactions were not my transactions. However, there was no information provided as—I do not shop at BJ's—there was no information provided as to how the breach happened, where it happened and to what extent the breach is.

In a lot of financial institutions, you have got sweep accounts, like a home equity credit account, that is tied into your checking account or an overdraft account, and there was no information given to me as to what the extent of the breach was.

Mrs. MCCARTHY. We as a committee usually do work very well together, but your input is going to be extremely important, because we are going to have to find a fine balance. But the more that you work with us—because a lot of us will come up with ideas that we find out later are not actually enforceable.

I found out from a lot of lobbyists, they said, "Well, we did not want to say it was not enforceable."

So it is important that you all work with us as we try and do it. Because it is going to be good for the consumer, it is going to be good for you. Because the more that we see this—the consumer is going end up paying for it one way or the other, in higher interest rates or any other thing.

I lost my wallet a couple of months ago, and being that I know what I know from this committee, I immediately reached out to everyone—because I keep photostatic copies of every charge card. Everything I have in my life is in a backup.

But what I forget about was that it would take months for someone to notify me, possibly, if something was being done. So I signed up for one of those credit cards from the banks, you know, for $10 a month they give me all the information I need. To me, it is worth $100 a year just to have that.

Mr. PRICE. The gentlelady's time has expired.

Mrs. MCCARTHY. Thank you.

Mr. PRICE. Thank you.

The Chair recognizes the gentleman from Mississippi, Mr. Lynch, for 5 minutes—Massachusetts, I am sorry.

Mr. LYNCH. Yes, Massachusetts. You would know by the accents.

[Laughter.]

Mr. PRICE. Well, I was going to say to Ms. McCarthy that a lot of committee members will have "idears" and a lot of them will have "ideas."

[Laughter.]

Mr. LYNCH. First of all, I want to thank the panel for helping the committee with its work.

Just as footnote to all of this, logistically, in our congressional offices, we typically deal with Social Security cases coming in the door, we deal with veterans' affairs and veterans' benefits—those are cases that we see on a regular bases. So we actually set our offices up to deal with, on a routine basis, those cases.

And recently in my office we have had to add somebody—not a full-time equivalency—but a person who is just designated to handling identity theft cases because they so frequent now, and we are seeing that played out in the press as well, but also because they are so difficult.

Many of these cases have wiped out constituents in my district completely, individuals, including businesses, and oftentimes the

theft occurs, the source of the theft is in another state. In one of our examples that we have dealt with there is a couple who own a business in Massachusetts who their identity was stolen in Arizona. We had to get the FBI involved.

But just as sort of a notice to you that congressional offices are becoming the repository of these cases. So I am sure that Congress will deal with this in some form in the immediate future.

Given the fact that these victims of identity theft—the consumers are blameless. They are innocent of any wrongdoing here. And yet, under the existing system, at least the cases that I have seen, they are being asked to bear the brunt of the burden of all of this.

It is their assets that are being stolen. These cases are very activity-intensive on the part of the victim. They have to go out there—it is a burdensome process to clean up identity theft, especially when there may be several possible sources of this, and they are getting very little help.

As I say, we have had to contact the FBI. We have had to try to marshal resources at the federal level to deal with this.

You know, I sort of got stuck on Mr. Foley's comments early about there are very few incentives or benefits to merchants to put the money in to properly protect that information.

And I am just thinking, this is getting worse. It is actually beginning to shake the confidence of the American consumer. And there might be a little bit of whistling to the graveyard here and not fully recognizing the damage that that would do if we shake consumer confidence to the level that people do not want to engage in e-commerce, do not believe that it is a safe transaction, many of the transactions they are making with their credit cards, that could be a tremendous damage to our economy.

So hearing all that, is there some way that we might bring some—and I recognize the need for a federal response here and perhaps federal preemption. Would you be willing to consider—and this is for the entire panel—enhanced penalties here for merchants who are reckless or negligent in handling personal information?

Would you support measures that would compensate the victims here for their loss, given the fact that they are not culpable in any way, they are blameless.

And given the obstacles to prosecuting a case on behalf of an individual, would you support a cause of action that would allow a private right of action, with attorney's fees, for consumers who are ripped off in this fashion?

Because I do not see a framework out there right now that would allow the rights of individual consumers to be protected. And we are seeing some huge numbers here in terms of identity theft, and these tapes going missing and data files being compromised.

It is a troubling situation, and we have to have some type of response to this besides just a notice. We have to have some recourse. And I think that that will put the fear of God into some people about the importance of protecting individual privacy rights.

I would like to hear from all of you. Thank you.

Ms. DESOER. At Bank of America, if I can start, a couple of things:

Number one, we have introduce something we call "total security protection" into all of our products so that our customers who are

a victim of fraud or unauthorized use of their accounts, they are reimbursed for any of their expenses.

We have also worked to your point of the confusion and the length of time of the situation to centralize the way we deal with a customer and their relationship with us. And as members of the Financial Services Roundtable, the industry has worked to build that kind of centralized place where we can have expertise at hand to deal with customers so it is sort of a one-stop place that they can go to get as much of the hard work that is involved in rectifying a situation done.

So for us, it is a combination of all the work that we have in progress to attempt to reduce the risk to our consumers, and then for consumers who are exposed to the risk to be able to simplify the process that they follow in contacting us and us working to help resolve the issues that are created by it.

And then, thirdly, there is no financial liability on any of our products and services.

Mr. FOLEY. Having personally been victimized, Congressman, I just hope that whatever we do applies retroactively so I could collect some of the money I lost trying to reestablish my own accounts and identity and the time that it took me to do that.

I would also add that——

Mr. LYNCH. Mr. Foley, on that point, I mean, you must have explored that possibility, right?

I mean, I know that for many of these identity theft victims, the only recourse that they have, generally, is to sue the merchant based on the merchant's own privacy policy. That seems to be the only common denominator. If it is cleverly crafted, that may be, you know, an empty opportunity as well.

Mr. FOLEY. Yes. As an individual, I still do not know how my information was breached, quite frankly. And I am very, very protective, being in the business that I am in.

I would also say, I was expert in terms of getting remedy and getting my funds back from the issuer as quickly as I possibly could. I do not think that most consumers would have that knowledge level that I had, to Congressman McCarthy's question.

It was about, all in all, about a 1-month process for me to complete all the paperwork and documentation to make sure that all the transactions were refunded to me.

In response to your question, I do agree with it.

I would say that the other piece of this that needs to be examined would be the people in the payment systems industry. My personal experience is mostly with MasterCard and Visa.

My hope would be that the private sector would be able to address this problem. And the credit union industry has had ongoing talks with MasterCard and Visa.

There are card association rules, which I believe will levy up to a $0.5 million penalty toward each merchant that was noncompliant with the standards. However, as I had said in my testimony, I have not seen much evidence of the card associations bringing any sort of standard to bear on behalf of the merchants.

So that I would just like to underscore, I think that as we go through this process, there also needs to be some redress for the people in the payment systems.

And also just to underscore, as a small issuer, the drain that it is bringing on the payment systems. When one of my member's accounts is cleaned out, they want their money back immediately. In my own case, I have two people that support 10,000 cards. And when one of these large breaches happens, 700 cards are stolen, I have two people that are immediately trying to deal with that issue, and every single one of those cardholders' issues is more important than the guy next to them.

So I think that it is important to also consider the whole role the payment systems plays in this issue.

Mr. PRICE. The gentleman's time has expired.

Would the remaining panel members wish to respond very briefly?

Mr. SANFORD. We agree that the time and intrusion on people's lives, if they are a victim, is significant. That is why we arranged for those counselors, that is why we got them insurance to compensate them for lost wages.

I think there is tort liability available for people. There already is a cause of action if they suffer actual harm.

I am not familiar with the regulatory framework for merchants, though, that might apply for these penalties.

Mr. LYNCH. So do you support an enhanced cause of action right now? It is very cumbersome for an individual to try to bring a cause of action for identity theft.

Mr. SANFORD. I actually did not know that it was difficult for them to bring cause of action.

Mr. PRICE. Mr. Ward, did you have a comment?

Mr. WARD. Yes. Actually, the battle against identity theft is really a two-prong battle. It is on the electronic side, which is what all the gentlemen on this panel were talking about. The other part of the battle is on the disposal side.

The disposal of information improperly accounts I have heard numbers from anywhere from 5 percent to 35 percent of the total identity theft problem.

If you can deal with that part of the issue—which can be dealt with fairly easily, fairly inexpensively—under the framework that you all have already established through the FACT Act, you can deal with some significant portion of the problem already.

Additionally, if you can put the management of these companies on notice through some type of Sarbanes-Oxley-type arrangement where they are held accountable and responsible for the development of a proper disposal plan, then that will put some teeth into it and should help alleviate some of the disposal issues.

Mr. LYNCH. Mr. McGuffey, should there be any—and I am just trying to get the final answer from the panelists. I mean, is there any value in holding these people accountable?

Mr. MCGUFFEY. Well, I have a similar reaction. First of all, we are not in the merchant business. And I would have thought that there was tort liability.

But your point of the amount of time and effort that individuals have to spend is one of the reasons that we funded a nonprofit organization, the Identity Theft Center, in order to help and provide assistance to where those who maybe do not know how to take care of these matters or have assistance, and it is expanding the victim

assistance that that particular nonprofit can deliver. It is launching consumer education and developing a panel of experts to be able to continuously improve the response and best practices associated with this.

So we recognize some of that, and we are trying to fund that effort in order to help victims.

Mr. PRICE. The gentleman's time has expired.

Mr. LYNCH. Thank you, Mr. Chairman.

Mr. PRICE. Thank you.

And I appreciate the indulgence of the committee members.

The Chair recognizes Ms. Wasserman Schultz from Florida for 5 minutes.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman. There is something to be said to saving almost the best for last.

The question that I have is actually related to legislation that you have referred to during your testimony that is being found around the country and the States. And we also, obviously, have four or five bills that I am aware of that have been filed here.

I guess the concern that I have is not providing, since we are talking about security, not providing consumers with a false sense of it. Because much of what your companies are doing, most people are not aware of. I mean, your processes by their very nature are very internal.

So what do you think the best approach is to ensuring that we are not regulating for regulations sake? I mean, you can write a law that requires you to reveal a breach. But let's say you do not. How are we going to ensure that we write a law that actually ensures, I mean, the ease of enforcement?

All of you can respond.

Ms. DESOER. In the financial services business, again, with the laws that do exist in the Interagency Guidelines, there is the office of the controller of the currency, who is the next line of defense to do that kind of audit to validate that we are in compliance.

And so I would think there would need to be something equivalent to that to ensure—I mean, we take the responsibility and accountability on ourselves as the first line of defense to comply, but there are second lines of defense and third line of defense and the regulators that do double check that we are compliant.

Ms. WASSERMAN SCHULTZ. But there is also—just before the rest of you answer—there is some moral obligation for you all to have reported breaches that occurred, and at least some of you waited a long time before you did that.

I mean, should there be a very significant—I mean, there has to be something that pokes beyond your conscience.

I mean, I am concerned that we would, in the rush to reassure our constituents that we are addressing this, that we will pass a whole lot of legislation that really will not make the situation better, because it will be extremely difficult to enforce and there will still be much of the obligation on you and that that is really the ultimate consumer protection.

Ms. DESOER. It really is. Because the first guiding principle needs to be that anyone who is in the business of collecting or storing or disposing of customer information takes their responsibility for safeguard that information very seriously.

If you do not start with that, you are right, you could get a false sense of security.

Mr. FOLEY. My particular experience is fairly specific. The credit and debit cards, in our case, quite frankly, because of our limited resources, it is more expensive for us to monitor accounts than it is just to automatically do a reissue and know that there is not going to be a problem further down the line.

So that in our particular case, although we are doing the notification, we are protecting the consumer by doing immediate reissue of the account so that there is no question 6 months down the line and we do not have the spend the resources for 6 months monitoring the account.

Like our counterparts in the commercial banking area, the National Credit Union Administration does require security audits, and most financial institutions, as a regulated industry, would have to comply with those federal audits.

Mr. MCGUFFEY. Earlier in the question and answer period here there was a question about market forces. And we happen to think that there are significant market forces that cause companies to do the right thing in order to protect data, in order to either notify, which as you know a number of us did, without a regulation.

It is difficult occasionally to write regulation, it would seem to me, and then also be able to deal with compliance aspects of it.

Indeed, we already are finding, I think as testimony has been given, that our law enforcement appears to somewhat underfunded in the ability to go and execute against the criminals who oftentimes appear to be winning.

So we have supported the law enforcement. We are in support of funding additional in order to make sure that we are able as a country and a society to catch the criminals, because ultimately we have to get rid of them in order to fix part of this problem.

Mr. SANFORD. I think if you have a statute, like take notice, clearly you have to put teeth into it to do your investigations in an expedient and reasonable fashion. You need to make notice in an expedient manner. I think the California statute has that language.

Certainly for people that violate that, if there is a penalty in the statute, I mean, that makes sense.

Less expedient—that is the question. Because every breach is going to be different, depending upon the number of individuals, the complexity of the breach, the sophistication of the company. Was the technology designed for that company such that it can recreate history to determine what happened?

So I think we are stuck with the fact that we have lots of different businesses out there.

But I do not want to lose sight of the fact that my company and every company in my industry is regulated by unfair and deceptive business practice statutes at both the federal and every state level. I mean, attorney generals in the States are very active. People look at businesses like us, when we do things voluntarily, to see whether or not we are being responsible businesses.

I do not think we can legislate this morality into businesses.

It is important to us, it is important to the 40,000 people that are part of my company around the world, that my company, when

it faces adversity, shows its true character and does what is responsible, whether there is a law or not.

And there are no laws guiding me in most of anything we have done in this manner.

And so what I have said is, I certainly would welcome the legislation if this committee deems it is appropriate, because we are doing these things anyway.

Mr. PRICE. Mr. Ward?

Mr. WARD. The key to a company properly disposing of their records is to do the due diligence with the contractor that they choose to have destroy their financial records or personal records.

Our industry has a voluntary self-imposed certification process through our trade association where we have gone through, and each company, member-company, is subject to an annual audit. And the annual audit has a pretty lengthy series of policies and procedures that if the company passes that audit then the contracting company who hires the shredding vendor should feel comfortable that that person is not going to willfully steal any of the information.

I cannot speak to mistakes, because those things do happen periodically.

But since our association has been formed 11 years ago, we have about 650 members in the association, and we have had no leaks of information under that process.

Mr. PRICE. The gentlelady's time is expired. Thank you.

The Chair recognizes the gentlelady from Wisconsin, Ms. Moore.

Ms. MOORE OF WISCONSIN. Well, thank you so much, Mr. Chairman.

And thank you, panel, for your patience.

I have questions that all of you can answer, because all of you seem to be very enamored with the idea of retaining the national I.D. number, or Social Security numbers, for just to have some sense of flow from one industry to the next.

It was 30 years ago, I knew people who were regarded as marginally saying, who, you know, were prophetic about the use of these Social Security numbers.

And, indeed, just a couple of weeks ago, a few weeks ago, I was cutting up old cards that were no longer useful and realizing that my health insurance card had my full Social Security number on it. I had been walking around with it in my pocketbook for 16 years. Both of my sons had one.

You know, every clerk, receptionist, temp worker that ever—you know, I understand electronic problems and disposal side problems.

But my Social Security number, the full Social Security number, was used as my member I.D. number.

So I think that people who are not hackers have access—you can barely check out of the hospital with a newborn without having a Social Security number. Somebody is born, and they have no way of protecting their identity.

Also, I guess this question is very directed toward Ms. Desoer—I hope I am pronouncing that correctly—or to Mr. Foley, who is with the Harvard University Employees Credit Union.

I recall—and I hope I am not preaching our confidentiality, Congresswoman Wasserman Schultz—as we were agonizing over

whether or not to vote for the bankruptcy bill, trying to just view it as a way of controlling all the slackers, that there absolutely was no protection, as has been discussed, for people whose identity is stolen.

I mean, they are people who would not necessarily have bankruptcy available to them, who are victims of identity theft.

So I guess, before my time expires, I would really like you guys to address those two things.

I mean, number one, you know, your Social Security number, it is for the convenience I think of these industries, is used everywhere, and we are required to carry these cards around in our pockets. It does not matter—you know, I am sitting here shredding it up after I have carried it in my wallet for 16 years, and my kids have lost them a thousand times.

And, also, why were you all so adamant about not protecting people whose identities were stolen in new bankruptcy bill?

Thank you.

Ms. DESOER. Related to the Social Security number and its use at Bank of America, we do use it as an identifying piece of information in order to validate and authenticate and identify the customer who is attempting to open a new account, attempting to obtain credit et cetera.

And then once we have obtained it, again, we take our responsibility to protect that information from getting in the wrong hands the wrong way accordingly by truncating numbers and other methods of protecting.

So we take that very seriously, and we believe we have the right processes in place to protect it.

On your issue relative to Social Security number and protections in bankruptcy, I need to get back to your office, I am sorry, with an answer to that question.

Ms. MOORE OF WISCONSIN. Okay, thanks.

And before my time expires, I do want to ask a very pointed question to ChoicePoint: You said in your press release and in your testimony today that ChoicePoint will discontinue the sale of information products that contain 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 support Federal, State or local government and criminal justice purposes.

My God, what exception is that? Sounds like it is wide open to me—that is in addition to the others I have asked.

Mr. FOLEY. I will just also echo that I am not as familiar with the bankruptcy provision. I will have to follow up with under what circumstances somebody would be able to be considered. I believe there are exclusions, but I am not sure of that.

In terms of financial institutions capturing and using the Social Security number, again, there are requirements for us to file information with the Internal Revenue Service, and we have for quite some time been masking and protecting that, no longer using that as part of the account number itself.

But at some point in that account opening, in order for us to comply with IRS reporting, we do need to capture it.

Mr. MCGUFFEY. Yes, we have had discussion around the use of Social Security numbers, and I agree with you, they are relatively prevalent and used as an I.D. oftentimes. Indeed, even in my past, my health care card had an I.D. number that was my Social Security number.

So Social Security numbers are used a great deal as an I.D. And in fact, it is used as one of the key identifiers to help make sure that we are associating a transaction or other records with the right person, making sure that we are not causing conflict with someone else because we are misusing a particular record because we do not have a good identifier.

So it is important to use those Social Security numbers and other identifiers to make sure that we are associating the proper records together.

With regard to our business changes that we have made, the business changes that we have made really isolate the use of and the display and the delivery back to our customers in situations where there is a consumer benefit.

Examples of that would be where an individual is seeking insurance, and in that situation they may disclose their Social Security number, we may need to be able to make sure that we are associating the proper records together, where we are actually providing to our customer the appropriate record so they can proceed and underwrite the business.

Preemployment screening is another line of service that we have that is covered by FCRA, as the insurance is, insurance services are, and in that case we oftentimes have to use a Social Security number to make sure that we are associating proper records, whether they may be a credit report, whether it may be a driver's license number in order to get a motor vehicle record, or in some cases even to make sure that we can identify the right person associated with a criminal record.

So there are a number of cases in our business that we will continue to use Social Security numbers, and most of those are transactions that are initiated by a consumer.

Mr. SANFORD. Decades ago the Social Security number——

Ms. MOORE OF WISCONSIN. Including the criminal, you know, like the woman who just got a mortgage recently in this area, stealing somebody's I.D. I mean, I walk in there with my health care card with my Social Security number on it, and there is a receptionist who can go file for a mortgage.

Mr. PRICE. The gentlelady's time has——

Ms. MOORE OF WISCONSIN. That is a consumer—I am sorry, Mr. Chair.

Mr. PRICE. It has expired. If you want to briefly answer, Mr. Sanford, Mr. Ward?

Mr. SANFORD. Yes, Mr. Chairman.

I mean, clearly, when Social Security numbers were introduced decades and decades ago, they were not intended to be national identification numbers. For good or bad, they are now in the public domain.

There was a Wall Street Journal article a few weeks ago that said you could do a Google search and pull up 70 million, I think was the number, of Social Security numbers.

The reason why a Social Security number is out there, why our industry is suggesting that we not limit access to it, is because of that unique ability to match and link data. There are people transacting today, doing business, using Social Security numbers that have not even been issued yet. And if we did not have SSNs, we could not match and link data to show that.

We have people using SSNs that are other people's. We have people using SSNs that do not match date of birth. We have people using SSNs and providing addresses which are prisons and hospitals, which are high-risk addresses, which indicate that there is a potential fraud associated with this particular individual. We have people using them on people who are deceased.

And so what we are saying is, is that leave the SSNs available to match and link data so we can stop the fraud. We maybe can do a better job on display, on who really needs to see it in the answer.

On bankruptcy, we did not weigh in on the debate on the bankruptcy legislation, so I am not able to respond to your question on that.

Mr. PRICE. Mr. Ward, briefly?

Mr. WARD. Thank you.

What your question points to is directly to the need for a consumer disclosure statement. If you go into your doctor's office and they ask for your health care card and it has your Social Security number printed on it and they photocopy it and later dispose of it, you have no clue or idea how that information has been disposed of.

With a proper disclosure statement, then you know what that company or doctor's office policy is toward disposal of that information and you know what procedures they go through so you can feel comfortable with releasing that.

Mr. PRICE. I want to thank the members of the panel for your patience and for your information and would encourage you, as others have, to continue to increase the communication with this committee as we move forward.

This hearing stands adjourned.

[Whereupon, at 12:46 p.m., the committee was adjourned.]

A P P E N D I X

May 4, 2005

Opening Statement

Chairman Michael G. Oxley

House Committee on Financial Services

Assessing Data Security:
Preventing Breaches and Protecting Sensitive Information

May 4, 2005

This morning, the Committee meets to consider a topic we've been hearing about on an almost daily basis during the past few months: data security and its connection to the crime of identity theft. Several recent high-profile security breaches have focused public attention as never before on the vulnerabilities of companies' data security systems. Congress now has to ask, "Are we doing enough to protect against the theft and misuse of sensitive commercial information on consumers?"

Protecting sensitive information is an issue of great importance for all Americans. In recent years, criminals in the United States and abroad have become increasingly inventive in finding ways to access and exploit information systems in order to commit identity theft.

According to a Federal Trade Commission estimate, over ten million Americans are victimized by identity thieves each year, costing consumers and businesses over $55 billion per year, not counting the estimated 300 million hours spent by victims trying to repair damaged credit records. The financial costs are staggering, with over $10,000 stolen in the average fraud.

The Financial Services Committee has worked tirelessly over the past several Congresses to identify and enact solutions to this destructive crime. During the 108th Congress, over 100 witnesses came before this Committee to testify on the reauthorization of the Fair Credit Reporting Act. Through that process, under the leadership of the gentleman from Alabama, Mr. Bachus, the Committee developed an exhaustive record on the need to increase safeguards designed to protect consumers and businesses alike from identity theft.

Through bipartisan cooperation in this Committee, we ultimately produced strong consumer protection and anti-identity theft legislation known as the Fair and Accurate Credit Transactions Act, or FACT Act.

The FACT Act places new obligations on financial institutions to prevent identity theft, entitles consumers to a free annual credit report from each of the three major credit bureaus, and creates a national fraud alert system to simplify a consumer's ability to detect and report fraudulent activity. The FACT Act was signed into law on December 4, 2003, and is currently in the process of being fully implemented by Federal regulators and the financial services industry.

The Federal banking regulators have also been hard at work on other initiatives to protect sensitive information. On March 29, 2005, the Federal Reserve, FDIC, OCC and OTS issued final data security standards for depository institutions, as required in Title V of Gramm-Leach-Bliley. The standards call for every financial institution to implement a response program to address incidents of unauthorized access to customer information maintained by the institution, and to notify the affected customer as soon as possible.

In light of continuing guidance from the regulators, it is my hope that we can focus today on the broader issue of data security, and how best to protect sensitive information from being improperly accessed, and ensure that consumers receive prompt and effective notice when sensitive information **has** been compromised and is likely to be misused. One of my concerns in this regard is that, given the dramatic rise in recent reports on data breaches, there will be a head-long rush toward notification in **every** instance.

When no evidence surfaces to indicate that their information has been misused, consumers may begin to ignore these notices as just that many more pieces of unsolicited junk mail.

California recently enacted legislation requiring disclosure of any data security breach to any state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Only a small percentage of these cases, however, have actually resulted in any fraudulent activity. Other States are considering legislation similar to California's. It is important that this Committee take a look at what is being contemplated in the States and consider whether a national breach notification standard would work best for American consumers.

I would like to welcome our witnesses to today's hearing. I look forward to hearing your testimony and working with you to find ways to prevent future data security breaches and continue our efforts to combat identity theft.

Statement of Congressman Michael N. Castle

Financial Services Committee Hearing on
"Assessing Data Security: Preventing Breaches and Protecting Sensitive Information"

May 4, 2005

Thank you Chairman Oxley and Ranking Member Frank for holding this important hearing today before the Financial Services Committee. In recent months, a number of "data breaches" have come to light. I think it is important we understand the situations surrounding each breach and learn how some of the companies testifying before us today took steps to remedy these situations.

Today, we live in a world that has become increasingly complicated and reliant on technology and dependent on data for instant decisions. Therefore, Mr. Chairman, I believe it is worthwhile for us to explore the practicality of requiring database security safeguards for most of the public and private sectors. While our financial institutions, as defined by the Gramm-Leach-Bliley Act, are already required to secure their sensitive data, it may be that we should do likewise across other sectors.

In the coming weeks, we are planning to introduce a comprehensive bill that, in part, requires many more databases to have a standard level of protection. In addition, we will define what constitutes a breach so that effected entities, regulators and consumers, can be notified when appropriate and in a coordinated manner. I am pleased to be working with the Gentlewoman from Ohio, Ms. Pryce, on this legislation that is intended to address a number of these and other concerns.

Finally, I am interested in hearing from our panelists about steps they took to ensure the future safety of the breached parties sensitive information. Some companies have provided free credit monitoring for all those that were subject to the breach. I think this is an enormously positive step that helps consumers and restores confidence and peace of mind to many.

The flow of information in our society is important -- it helps consumers everyday with access to credit, price competition, and even with issues related to public safety. Mr. Chairman, I thank you for holding this hearing today and I look forward to hearing from each of our witnesses.

OPENING REMARKS OF THE HONORABLE RUBEN HINOJOSA
HOUSE COMMITTEE ON FINANCIAL SERVICES
"ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION"
MAY 4, 2005

Chairman Oxley and Ranking Member Frank,

I want to express my sincere appreciation for you holding this very important and timely hearing today. Having served as one of the Members of the Task Force on Identity Theft that contributed substantially to the language ultimately included in the FACT Act of 2003, I am very disturbed by the recent events that have endangered the personal privacy of many of our constituents, including over 300,000 in the Lexis-Nexis case alone.

For weeks, the media has reported on the rampant loss of financial information of Americans from coast to coast. What at first seemed to be isolated incidents of theft now seems much larger and has impacted customers of well-known companies like Ralph Lauren, DSW Shoes, Lexis-Nexis, and others. The frightening part of this lapse in security is that millions upon millions of people are now exposed to possible identity theft.

Identity theft can be devastating for consumers and can destroy their credit, their financial security and their sense of protection and well-being. Similar to a home invasion or robbery, victims of identity theft are exposed to the whims of those who stole their personal financial information. Identity theft tends to occur when an imposter steals a victim's personal information to gain credit, merchandise and/or services in the victim's name. It is the most common complaint received from consumers in all 50 states; and, my home state of Texas ranks third in the number of identity theft victims.

According to the Federal Trade Commission, identity theft occurs when an individual's Social Security number, credit card number(s), or name is used without permission or knowledge. Perpetrators of identity theft often use this information to open credit card accounts, utility services, or to use already existing accounts.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves have made to their good name. Victims of identity theft may incur unauthorized charges to their credit cards and unauthorized withdrawals from bank accounts. Victims may lose job opportunities, be unable to secure a loan, obtain a mortgage, or get arrested for crimes they didn't commit.

What's more frightening, is this crime often goes undetected. Most people aren't aware that they may have been victimized and that their accounts have been compromised until it's too late.

While it could be quite difficult to determine if you have been a victim of identity theft, there are a few warning signs. You may fail to receive bills or other mail, receive credit cards you didn't apply for, or receive calls from creditors or businesses about merchandise you didn't order or request. You can request, once annually, a free copy of your credit report, which contains vital information about your credit history. This new benefit is being implemented on a rolling basis.

As a member of the House Task Force on Identity Theft and co-founder and co-chair of the Financial and Economic Literacy Caucus, it is a priority for me to educate consumers about this very important issue – especially in light of these recent news reports. Many Americans are not aware of their rights and do not have a grasp of their own personal finances; thus, making them vulnerable to identity theft. I have been encouraging my constituents to begin taking the necessary steps to educate themselves about everything from how to fill out a loan application to understanding their own credit report.

However, I keep stressing that they do not have to sit idly by – they can prevent identity theft. They can tear or shred their receipts, copies of credit applications or offers, insurance forms, check and bank statements, and expired credit cards; keep their Social Security card in a safe place, and give their number only when necessary; pay attention to their billing cycles; do not write their PIN numbers on their credit or debit card; and, ensure that information they share on the Internet is with a legitimate institution or vendor.

And if they happen to find themselves a victim of identity theft, there are steps they can take immediately. Contact the fraud department of one of the three major credit bureaus – Experian, TRW, and TransUnion. As soon as the credit bureau they contact confirms the fraud alert, the other two credit bureaus will be automatically notified, and all three credit reports will be sent to the victim immediately. In addition, they should also close all tampered accounts, file a police report and file a complaint with the Federal Trade Commission.

I have informed my constituents that, for more information on what they can do if they believe their identity has been compromised, contact their local authorities or the Federal Trade Commission at (877) 438-4338 or www.consumer.gov/idtheft.

The Department of Justice www.usdoj.gov/criminal/fraud/idtheft/html and/or

BITS Financial Services Roundtable www.bitsinfo.org/ci_identity_theft.html

The purpose of today's hearing is to examine a number of recent data security breaches to determine how consumers' personal and financial information was stolen and what actions have been taken to minimize unauthorized use of the stolen information. The first thing we need to know are the facts surrounding the breaches.

According to Committee staff and to various press reports and press releases from the underlying entities, data thieves employed a variety of means to gain unauthorized access

to consumers' private information. These include both high-tech means for stealing computer access codes and passwords, as illustrated in the various university and retail store security breaches, as well as such low-tech methods as impersonating legitimate business clients, as in the ChoicePoint and Lexis-Nexis examples. Other security breaches involved more traditional forms of theft, such as the theft of computers and computer backup tapes in the Wells Fargo Mortgage and Bank of America examples.

The largest known security breach of financial data became public in February 2003 when the FBI announced a nationwide investigation of a breach of a computer database containing roughly 8 million Visa, MasterCard and American Express credit card numbers.

Officials of British-based HSBC PLC notified at least 180,000 credit card customers in mid-April 2005 that their account information may have been obtained in a security breach of the computer database of a national retailer.

DSW announced in April, 2005, that computer hackers had obtained account data from 1.4 million credit cards used by customers at 108 retail stores between November 2004 and February 2005. Checking account numbers and driver's license numbers where also stolen from nearly 95,000 customer checks.

Lexis-Nexis Group announced in mid-April 2005 that files containing social security numbers, driver's license numbers and other detailed personal information on 310,000 consumers had been illegally obtained by persons posing as legitimate business customers.

Officials of the University of California-Berkeley announced in April 2005 that a laptop computer containing information on 98,000 students and alumni had been stolen a month earlier. The computer contained unencrypted personal information including social security account numbers, birth dates and home addresses.

In March 2005, Boston College notified 106,000 alumni that a hacker had gained access to a computer database containing their personal information.

In February 2005 Bank of America announced that it lost computer backup tapes containing personal information, including social security account numbers and credit card accounts data, relating to 1.2 million federal workers, including many Senate office accounts.

The Chief Executive of Georgia-based ChoicePoint Inc. announced in mid-February 2005 that criminals posing as legitimate small businesses had obtained sensitive personal information on 145,000 American consumers during the summer and fall of 2004 and that at least 750 of them had been defrauded.

As a result of these thefts, several bills related to identity theft have been introduced during the 109th Congress.

H.R. 1099, the "Anti-Phising Act of 2005", would make it a federal crime to knowingly create or procure the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate online business; and use that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another. It would also be a crime to send a message that falsely represents itself as being sent by a legitimate online business for the purposes listed above. The penalty for each could be a fine, imprisonment for five years, or both.

H.R. 1078, the "Social Security Number Protection Act of 2005", would direct the Federal Trade Commission to promulgate regulations to impose restrictions and conditions on the sale and purchase of social security numbers.

H.R. 220, the "Identity Theft Prevention Act of 2005", would repeal provisions of the Social Security Act authorizing various uses of the social security number. The bill would also require all social security numbers to be randomly generated, make the social security number the property of the individual to whom it is issued, and prohibit the Social Security Administration from disclosing the number to any agency or instrumentality of the federal or state government. The federal government would also be prohibited from issuing government-wide identifying numbers or establishing a uniform standard for identification of an individual that is required to be used by any other federal agency, state agency, or private person.

Although the federal financial regulatory agencies and credit-card industry have been attempting to find ways to address the security breaches, I believe that additional hearings are needed to review the effectiveness of the identity theft provisions set forth in the FACT Act and to oversee the regulatory agencies' implementation of those provisions. I am not certain that legislation, such as that cited above, is needed at this time to address the current security breaches. However, I think that this Committee needs to continue its oversight role and to remain vigilant to ensure that we do all in our power to ensure that consumers' identities are not stolen, and, if they are, to provide the fastest remedy possible.

I look forward to the testimony of today's witnesses, and I yield back the remainder of my time.

COMMITTEE ON TRANSPORTATION
AND INFRASTRUCTURE
CHAIRMAN, SUBCOMMITTEE ON RAILROADS

COMMITTEE ON
FINANCIAL SERVICES

COMMITTEE ON
GOVERNMENT REFORM

Steven C. LaTourette
Congress of the United States
14th District, Ohio

May 4, 2005

Statement of Congressman Steven C. LaTourette
Hearing entitled, "Assessing Data Security: Preventing Breaches and Protecting Sensitive Information"

Mr. Chairman, thank you for holding this timely hearing. Quite frankly, it's unfortunate that we are here today. While I don't think any of us here were ever under the assumption that the good work we did when we reauthorized FCRA last Congress was going to be the panacea that put an end to skyrocketing reports of identity theft, I know I for one could not have envisioned the rash of data breaches that have grabbed the headlines over the last several months, cumulatively putting millions of American consumers at risk for identity theft.

We're here today to review a number of cases where criminal activity, simple negligence, inadequate security and fraud prevention procedures, or some combination of the three, facilitated the loss or compromise of personal data. While I do believe it is valid to find a method of determining the potential risk involved with a data breach, taking into account the type and nature of the incident, this Committee and the witnesses before us today must understand that we should not be focusing solely on reactionary measures. In my mind, if a breach of a database leads to even one identifiable case of identity theft, then existing regulation has failed and no number of mandatory notices – one hundred or ten million – is going to erase the damage that was already done. The challenge is now on us to find a balance that provides proactive fraud and database breach prevention, coupled with what should be a "worst-case" option of sending out mass mailings.

It is my hope that a bipartisan group of my colleagues from this Committee can come together to craft a bill that makes mandatory notification in cases such as these a federal requirement. That seems a practical step in light of what has happened. However, too often the old adage holds true that legislative bodies wait for catastrophe to strike before actually taking action. More needs to be done, and I intend to explore a variety of options that can give consumers options to protect their financial and personal data.

Thank you, Mr. Chairman.

ROOM 2453
RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-5731

1 VICTORIA PLACE
ROOM 320
PAINESVILLE, OH 44077
(440) 352-3939
TOLL FREE IN OHIO
1-800-447-0529

MORELAND HILLS VILLAGE HALL
4350 SOM CENTER ROAD
MORELAND HILLS, OH 44022
(440) 542-9300

P.O. BOX 1132
TWINSBURG, OH 44087
(330) 425-9291

Barbara Desoer
Global Technology, Service & Fulfillment Executive
Bank of America

Written Testimony to the Financial Services Committee of the United States House of Representatives Public Hearing to Assess Data Security
Washington, D.C.
May 4, 2005

Chairman Oxley, Congressman Frank, Committee Members, good morning.

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 the loss of computer backup data storage tapes reported by Bank of America earlier this year.

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 remarks today, I will provide an overview of:

1. What we know regarding the loss of our computer data backup tapes;
2. The steps we have taken to alert and protect our government charge cardholders;
3. Our information security practices; and,
4. 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 non-sensitive, back-up 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 were 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 GSA management and us 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. Following our initial cardholder notifications mentioned earlier, we continued to communicate with our customers to ensure they understood the additional steps we continue to take today to help protect their personal information and to assist them with any questions they have. With multiple mailings to cardholders with information on the tapes, this amounted to several million pieces of mail.

As part of our initial communications to cardholders, Bank of America also quickly established a toll-free number government charge cardholders could use to call with questions or request additional assistance. We 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've 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 (such as the BASEL II accord and international standards for information security controls). 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'd 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're 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. Within Bank of America, we have taken recent steps to further safeguard the secure transport of customer data, including the launch of corporate-wide package delivery carrier services for backup data tape transport.

We also acknowledge that in today's environment, in which information security issues or concerns are highly visible, there is a general belief that something must be done. I would like to assure the committee that things are indeed being done, and speaking for Bank of America, that we consider information protection among the highest priorities at our company and we take our responsibility for safeguarding it very seriously. Our annual investment in information security technology, personnel and assessment requires significant financial resources, however, it is an investment we make without hesitation and as tangible proof of the seriousness with which we treat our responsibilities.

With respect to legislative solutions currently under discussion, our recent actions demonstrate our belief that customers have a right to know when there is reason to believe that 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. In fact, our actions in this instance actually went beyond the scope of requirements that existed at that time.

Furthermore, our approach and existing policies and practices also are in accordance with the recently issued Interagency Guidance. We believe this guidance strikes the correct balance with respect to when notification is appropriate and what steps should be taken when a security breach has put a customer's personal information at risk. We also believe that a national approach to information security guidelines will promote the most consistent and efficient path to ensuring customer information privacy is maintained.

As the legislative process moves forward to determine the appropriate protections for consumers, we firmly believe it should support the following principles:

- Any business dealing with a customer's personal information has a duty to take all necessary steps to ensure the safety and privacy of that information is maintained.
- Consumers should be notified in a timely manner about any incident that could reasonably lead to the unauthorized use of their confidential information.
- Customer accounts should be monitored for fraudulent activity upon discovery of a potential security breach.
- Institutions and law enforcement must be permitted the opportunity to conduct appropriate investigations in advance of any notice.
- Institutions should protect their customers from any adverse impact from an incident and assist those who are adversely impacted with their recovery.

We believe these general principles are manifested in our actions and they are principles by which we will abide in the future. Our relationship with our customers is built on trust and our actions must always be guided by that bond.

We believe public-private partnerships to advance the cause of information security in this country are critical. We have always maintained that both government and industry have a role to play. We have actively participated in such partnerships and leveraged these working relationships over the past several years with extremely positive results.

In our experience, the best solutions often arise out of the work we do together, implemented through the voluntary cooperation of private sector organizations. The information security environment is by its very nature fluid and rapidly evolving, and demands solutions and counter-measures that can evolve and advance with speed and flexibility.

We look forward to helping promote that speed and flexibility and to taking part in the ensuing legislative dialogue. We also appreciate opportunities such as my appearance before the committee today to share our experience and opinions on such an important matter to our country, its financial systems and consumers.

Members of the committee, on behalf of our leadership team and all Bank of America associates, I can assure you that we will do all we can to make certain 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 be happy to answer any questions.

WRITTEN TESTIMONY OF EUGENE FOLEY
PRESIDENT AND CEO OF HARVARD UNIVERSITY EMPLOYEES
CREDIT UNION

ON

"ASSESSING DATA SECURITY: PREVENTING BREACHES AND
PROTECTING SENSITIVE INFORMATION"
BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES
MAY 4, 2005

WRITTEN TESTIMONY OF EUGENE FOLEY
PRESIDENT AND CEO OF HARVARD UNIVERSITY EMPLOYEES CREDIT UNION
ON
"ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION"
BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES
MAY 4, 2005

Mr. Chairman, members of the committee; my name is Eugene Foley and I am the President and CEO of Harvard University Employees Credit Union, located in Cambridge, Massachusetts. I am here today to express concern about the implications and escalating problem that theft of sensitive information resulting from data security breaches is having on American consumers, credit union members, and the institutions that issue credit cards and debit cards, most especially credit unions and small banks. Collectively, about 4,600 credit unions in this country have issued and support over 12.5 million card accounts for our members.

I have experience with this issue not only as the CEO of a credit union that had about 700 of our 10,000 card accounts compromised in one incident last year, but also as a recent victim of identity theft myself. While I was sitting in my office, with my own debit card securely in my wallet, my checking account was cleaned out by a series of card purchases made 3,000 miles away. In a matter of minutes, over $2,000 was stolen from my account. Given my position, I am particularly responsive in protecting my own sensitive information, but this caution is meaningless when entities that have captured and retained the data contained on the card stripe are careless or not compliant with security standards.

The frequency of major card data compromises is increasing at an alarming rate. Within the past two weeks alone, we have read of three major breaches which have compromised the accounts of millions of American consumers. The first major security breach to have an impact on credit unions came to light last year as result of hackers stealing a large amount of consumer information from the retailer, BJ's Wholesale Club. This case exemplifies a merchant in direct violation of card association rules and regulations. While card issuers fastidiously comply with protecting sensitive account data, the resources they expend in this effort are squandered if merchants are not held to the same standard.

A recent article in the *Wall Street Journal* cited a $5.7 million lawsuit filed last month against BJ's Wholesale Club by CUNA Mutual Insurance Corporation on behalf of 163 credit union bond holders. Millions of dollars were lost by credit unions in the security breach at BJ's alone. These costs include not only the amounts lost to fraud, but also the

costs for reissuing and blocking cards, for notifying card holders and monitoring accounts. There are card association rules in place regulating how the consumer

information which is imbedded on the magnetic stripe on the back of each card should be handled, but these rules have proven to be both insufficient and laxly enforced. Absent card association enforcement or legislative redress, credit unions have had to resort to litigation in order to find remedy for these losses.

The surest way to limit the potential damage when a merchant's files are hacked and a large base of credit card information is stolen is to cancel the existing cards and reissue new cards with new account numbers. As small banks and credit unions hold a close relationship with their card holders, this is most often the action they take. This is a very costly and time consuming undertaking. Unfortunately protecting the consumer also carries another very substantial penalty by causing the consumer to question the safety and security of the card issuer rather than the merchant who has inadequately safeguarded their personal information. The card issuer is unfairly exposed to the majority of this "reputation risk" in addition to actual monetary costs.

Even after a breach has been identified by the merchant, issuing institutions can not count on getting accurate and timely notification to pass along to the consumer. Most times, the issuer is relying on reports in the media to determine the nature of the breach. Without accurate information, it is impossible to appropriately inform our members how their information was stolen and they are often left with the impression that the credit union is at fault.

The California General Assembly undertook steps to provide this type of protection in a law that became effective on July 1, 2003. While we have had the benefit of seeing that law in action for nearly two years and their experience offers us some guidance, there is room for improvement.

It is our hope that the committee will put its authority and energy behind initiatives that will require the major credit card companies to notify financial institutions immediately in an electronic format that is usable for the effected issuer. That information should include: when a breach occurred, which merchant is responsible for that breach and which accounts are affected. It should also detail what type of personal information was compromised.

Specifically, any new statute would benefit from explicit definitions. For example, clarity with regard to which businesses would be covered, along with what constitutes personal information, are areas where the California statute has been questioned. Of particular concern is an exclusion that the California law provides for encrypted data. Unfortunately advances in hacking seem to match advances in encryption technology and those that can breach credit card files are quite likely to be able to gain access to decryption technology.

In addition, to ensure that all consumers have the utmost protection from this insidious threat, we believe that all credit card issuers should be required to at least inform consumers when their credit card has become compromised and their personal financial information has been stolen. Those consumers should then have the right to determine if they wish to have their cards cancelled and reissued, in a timely fashion, at no cost.

Mr. Chairman and members of the committee, I thank you for affording me the opportunity to share my thoughts on this subject with you.

Testimony of Don McGuffey
Senior Vice President for Data Acquisition and Strategy, ChoicePoint
Before the House Committee on Financial Services
May 4, 2005

Chairman Oxley, Ranking Member Frank and members of the Committee,

Good morning, I am Don McGuffey, Senior Vice President for Data Acquisition and Strategy of ChoicePoint. I have been with the company since its inception in 1997.

ChoicePoint has previously provided Congress with testimony about the recent illegal data access and the criminals who perpetrated this fraud, the steps we are taking to protect affected consumers, and the measures that we are taking to prevent similar violations from occurring in the future. While I have described the company's actions in my written statement to the Committee, I would like to specifically offer a sincere apology on behalf of ChoicePoint to those consumers whose information may have been accessed by the criminals who perpetrated this fraud.

What I hope you see in ChoicePoint is a company that has listened – to consumers, privacy experts and government officials – and learned from this experience. Accordingly, we have responded rapidly and in fundamental ways.

We have provided benefits to potentially affected consumers that no other information company had done before and that several companies have since emulated – including voluntary nationwide notification, dedicated call centers and Web sites, free three-bureau credit reports and one year of credit monitoring at our cost.

We learned that there are few places for consumers to turn for help if their identity is stolen. This alone increases the fear and anxiety associated with identity theft. For this reason, we have recently formed a partnership with the Identity Theft Resource Center – a leading and well respected non-profit organization dedicated exclusively to assisting identity theft victims.

Our partnership includes a $1 million cash contribution from the ChoicePoint Foundation and will help the ITRC serve consumers in the following three ways:

- Expand the victim's assistance program, which offers personal assistance to all current and potential victims of identity theft;
- Launch a consumer education and awareness campaign; and
- Participate in and advise a national working group with representation from across industry participants that will develop these best practices.

We've also hired Carol DiBattiste to serve as our first chief credentialing, compliance and privacy officer. This office will oversee the improvements in our customer credentialing process, the expansion of our site-based verification program and the implementation of an enhanced incident reporting procedure. Carol comes to us after a distinguished government career that includes key prosecutorial roles in the Departments of Defense and Justice as well as policy and senior leadership positions in the Departments of Homeland Security, Defense and Justice.

We have also appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the federal government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials. In his role, he will work aggressively to assist law enforcement in prosecuting those committing identity theft. Bob will also help us to ensure that our security and safeguard procedures continue to evolve and improve.

Just as criminals are ever diligent about finding new ways to evade procedures, we must be equally dedicated to staying ahead of those who would break the law. We have already made broad changes to our products – including limiting the distribution of personally identifiable information – and more changes are still under development. For example, ChoicePoint has decided to discontinue the sale of information products that contain personally identifiable

information, including Social Security and driver's license numbers, except when the products meet one of three very specific needs:

- The product supports consumer-driven transactions where the data is needed to complete or maintain relationships such as insurance, employment and tenant screening, or provides consumers with access to their own data;
- The product provides authentication or fraud prevention tools to large, accredited corporate customers where consumers have existing relationships. For example, information tools for identity verification, customer enrollment and insurance claims; or
- When personally identifiable information is needed to assist federal, state or local government and criminal justice agencies in their important missions.

Enabling business to mitigate fraud remains a key benefit of what we do, but is not our primary focus.

Most importantly, we have shifted our focus to ensuring our products and services provide a direct benefit to consumers or to society as a whole. While this has meant exiting an entire market, we decided that consumer interests must come first.

Mr. Chairman, before delving into the specifics of various policy proposals, perhaps it would be helpful if I gave members of the Committee, a brief overview of our company, the products we provide and some insight as to how we are currently regulated.

The majority of transactions our business supports are initiated by consumers. Last year, we helped more than 100 million people obtain fairly priced home and auto insurance, more than seven million Americans get jobs through our pre-employment screening services, and we helped more than one million consumers obtain expedited copies of their family's vital records – birth, death and marriage certificates. These transactions were started by consumers with their permission, and they provide a clear, direct benefit to consumers.

Not all of our other work is as obvious -- but the value of it is. At a time when the news is filled with crimes committed against children, we're helping our nation's religious institutions and youth-serving organizations protect those in our society who are least able to protect themselves. Our products or services have identified 11,000 undisclosed felons among those volunteering or seeking to volunteer with children --- 1055 with convictions for crimes against children. Forty-two of those felons were registered sex offenders.

Consumers, businesses and non-profits are not the only ones that rely on ChoicePoint. In fact, government officials have recently testified to Congress that they could not fulfill their missions of protecting our country and its citizens without the help of ChoicePoint and others in our industry. Last month, ChoicePoint supported the U.S. Marshall Service's in Operation Falcon, which served approximately 10,000 warrants in a single day for crimes ranging from murder to white collar fraud.

Mr. Chairman, apart from what we do, I also understand that the Committee is interested in how our business is regulated at both the federal and state level. The majority of our products are already governed by the FCRA and other federal and state laws including the recently enacted companion FACT Act, the Gramm-Leach-Bliley Act (GLB), the Drivers Privacy Protection Act (DPPA) as well as state and federal "do not call" and "do not mail" legislation. We believe consumers benefit from these regulations.

- 60 percent of ChoicePoint's business is driven by consumer initiated transactions, most of which are regulated by the FCRA. These include pre-employment screening, auto and home insurance underwriting services, tenant screening services, and facilitating the delivery of vital records to consumers.
- Nine percent of ChoicePoint's business is related to marketing services, none of which include the distribution of personally identifiable information. Even so, we are regulated

by state and federal "do not mail" and "do not call" legislation and, for some services, the FCRA.

- Five percent of ChoicePoint's business is related to supporting law enforcement agencies in pursuit of their investigative missions through information and data services.
- Six percent of our business supports law firms, financial institutions and general business to help mitigate fraud through data and authentication services.
- The final 20 percent of our business consists of software and technology services that do not include the distribution of personally identifiable information.

While a small percentage of our business is not subject to the same level of regulation, we believe additional regulation will give consumers greater protections. I therefore want to state for the record, ChoicePoint's positions on future regulation of our industry.

- We support independent oversight and increased accountability for those who handle personally identifiable information, including public records. This oversight should extend to all entities including public sector, academic and other private sector organizations that handle such data.
- We support a preemptive national law that would provide for notification to consumers and to a single law enforcement point of contact when personally identifiable information has fallen into inappropriate hands; ensuring that the burden of notice follows the responsibility for breach and that consumers do not become de-sensitized to such notices.
- ChoicePoint supports providing consumers with the right to access and question the accuracy of public record information used to make decisions about them consistent with the principles of FCRA. There are technical and logistical issues that will need to be solved, but they are solvable.

- We have already taken steps to restrict the display of full social security numbers and would support legislation to restrict the display of full social security numbers modeling existing law including GLB and FCRA while extending those principles to public record information.

We have all witnessed the significant benefits to society that can come with the proper use of information. But we have been reminded, first-hand, the damage that can be caused when people with ill intent access sensitive consumer data.

As a company we have rededicated our efforts to creating a safer, more secure society. We look forward to participating in continued discussion of these issues and would be pleased to answer any questions you might have.

Before the
U.S. House of Representatives
Committee on Financial Services

Hearing on
Assessing Data Security:
Preventing Breaches and Protecting Sensitive Information
May 4, 2005

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

Introduction

Good morning. My name is Kurt Sanford. I am the President and Chief Executive Officer for Corporate and Federal Markets at LexisNexis. I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the protection of consumer information.

LexisNexis is a leading provider of authoritative legal, public records, and business information. Today, over three million professionals—lawyers, law enforcement officials, government agencies employees, financial institution representatives, and others—use the LexisNexis services. Government agencies, businesses, researchers, and others rely on information provided by LexisNexis for a variety of important uses.

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

Preventing identity theft and fraud – Although the insidious effects of identity theft are fairly well known, until recently we did not fully appreciate that identity theft is part of the larger problem of identity fraud. Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It is a component of most major crimes and is felt around the world today. As a result, both industry and government have asked LexisNexis to develop solutions to help address this evolving problem.

LexisNexis remains committed to providing leadership in this area. We recognize the enormity of the problem. In 2004, 9.3 million consumers were victimized by identity fraud. Credit card companies report $1 billion in losses each year from credit card fraud. With the use of a LexisNexis solution called Fraud Defender, a major bank card issuer experienced a 77 percent reduction in the dollar losses due to fraud associated with identity theft and credit card origination.

LexisNexis products are becoming increasingly necessary to combat identity fraud associated with internet transactions where high dollar merchandise such as computers and other electronic equipment are sold via credit card. Lower fraud costs ultimately mean lower costs and greater efficiencies for consumers.

Preventing money laundering – LexisNexis has partnered with the American Bankers Association to develop a tool used by banks and other financial institutions to verify the identity of new customers to prevent money laundering and other illegal transactions used to fund criminal and terrorist activities. This tool allows banks to meet Patriot Act and safety and soundness regulatory requirements.

Locating suspects and helping make arrests – Many federal, state and local law enforcement agencies rely on LexisNexis to help them locate criminal suspects and to identify witnesses to a crime. LexisNexis works closely with federal, state and local law enforcement agencies on a variety of criminal investigations. For example, the Beltway Sniper Task Force in Washington, D.C., used information provided by LexisNexis to help locate one of the suspects wanted in connection with that case. In another case, information provided by LexisNexis was

recently used to locate and apprehend an individual who threatened a District Court Judge and his family in Louisiana.

Supporting homeland security efforts - LexisNexis worked with the Department of Homeland Security Transportation Safety Administration (TSA) in developing the Hazardous Materials Endorsement Screening Gateway System. This system allows TSA to perform background checks on commercial truck drivers who wish to obtain an endorsement to transport hazardous materials.

Locating and recovering missing children – Customers like the National Center for Missing and Exploited Children rely on LexisNexis to help them locate missing and abducted children. Since 1984, the Center has assisted law enforcement in recovering more than 85,000 children. Over the past 4 years, information provided by LexisNexis has been instrumental in a number of the Center's successful recovery efforts.

Locating parents delinquent in child support payments – Both public and private agencies rely on LexisNexis to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for the Enforcement of Support (ACES), a private child support recovery organization, has had tremendous success in locating nonpaying parents using LexisNexis.

These are just a few examples of how our information products are used to help consumers by detecting and preventing fraud, strengthening law enforcement's ability to apprehend criminals, protecting homeland security and assisting in locating missing and abducted children.

Types of Information Maintained by LexisNexis Risk Solutions

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

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

Publicly available information. Publicly available information is information that is available to the general public from non-governmental sources. Telephone directories are an example of publicly available information.

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

Privacy

LexisNexis is committed to the responsible use of personal identifying information. We have privacy policies in place to protect the consumer information in our databases. Our Chief Privacy Officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong privacy policies in place to help protect the information contained in our databases. We also undertake regular third-party privacy audits to ensure adherence to our privacy policies.

LexisNexis has an established Consumer Access Program that allows consumers to review information on them contained in the LexisNexis system. While the information provided to consumers under this program is comprehensive, it does not include publicly available information such as newspaper and magazine articles and telephone directories contained in the LexisNexis system.

LexisNexis also has a consumer opt-out program that allows individuals to request that information about themselves be suppressed from selected databases under certain circumstances. To opt-out of LexisNexis databases, an individual must provide an explanation of the reason or reasons for the request. Examples of reasons include:

- You are a state, local or federal law enforcement office or public official and your position exposes you to a threat of death or serious bodily harm;
- You are a victim of identity theft; or
- Your are at risk of physical harm.

Supporting documentation is required to process the opt-out request. While this opt-out policy applies to all databases maintained by our recently acquired Seisint business, it is limited

to the non-public information databases in the LexisNexis service. The policy does not currently apply to public records information databases maintained by LexisNexis. We are currently evaluating what steps we can take to better publicize our opt-out program and extend the program to all public records databases in the LexisNexis service.

Security

LexisNexis has long recognized the importance of protecting the information in our databases and has multiple programs in place for verification, authorization and IT security. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities. LexisNexis also has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information contained in our systems. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials. We also authenticate the documents provided to us to ensure they have not been tampered with or forged.

Only those customers with a permissible purpose under applicable laws are granted access to sensitive data such as driver's license information and social security numbers. In addition, customers are required to make express representations and warranties regarding access and use of sensitive information and we limit a customer's access to information in LexisNexis products according to the purposes for which they seek to use the information.

Maintaining security is not a static process -- it requires continuously evaluating and adjusting our security processes, procedures and policies. High-tech fraudsters are getting more sophisticated in the methods they use to access sensitive information in databases. We

continuously adapt our security procedures to address the new threats we face every day from those who seek to unlawfully access our databases. We undertake regular third-party security audits to test the security of systems and identify any potential weaknesses.

Even with the multi-layer safeguards in place at LexisNexis, we discovered earlier this year that unauthorized persons primarily using IDs and passwords of legitimate customers may have accessed personal identifying information at our recently acquired Seisint business. In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. At that point we contacted the U.S. Secret Service. The Secret Service initially asked us to delay notification so they could conduct their investigation. About a week later, we publicly announced these incidents and within a week sent out notices to approximately 30,000 individuals.

The investigation revealed that unauthorized persons, primarily using IDs and passwords of legitimate customers, may have accessed personal-identifying information, such as social security numbers (SSNs) and driver's license numbers (DLNs). In the majority of instances, IDs and passwords were stolen from Seisint customers that had legally permissible access to SSNs and DLNs for legitimate purposes, such as verifying identities and preventing and detecting fraud. No personal financial, credit, or medical information was involved since LexisNexis and Seisint do not collect such information. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated nor was any customer data residing within that infrastructure accessed or compromised.

Based on the incidents at Seisint, I directed our teams to conduct an extensive review of data search activity at our Seisint unit, and across all LexisNexis databases that contain

personal identifying information. In this review, we analyzed search activity for the past twenty-seven months to determine if there were any other incidents that potentially could have adversely impacted consumers. We completed that review on April 11, 2005. As a result of this in-depth review, we discovered additional incidents where there was some possibility that unauthorized persons may have accessed personal identifying information of approximately 280,000 additional individuals.

We deeply regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify the identified individuals. We are providing all individuals with a consolidated credit report and credit monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity. We will also provide them with identity theft expense insurance coverage up to $20,000 to cover expenses associated with restoring their identity and repairing their credit reports.

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

- Changing customer password security processes to require that passwords for both system administrators and users be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;

- Suspending customer passwords after five unsuccessful login attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation;
- Further limiting access to the most sensitive data in our databases by truncating SSNs displayed in non-public documents and narrowing access to full SSNs and DLNs to law enforcement clients and a restricted group of legally authorized organizations, such as banks and insurance companies; and
- Educating our customers on ways they can increase their security.

Laws Governing LexisNexis Compilation and Dissemination of Identifiable Information

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

The Gramm-Leach-Bliley Act. Social security numbers are one of the two most sensitive types of information that we maintain in our systems and credit headers are the principal commercial source of social security numbers. Credit headers contain the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, social security number, and month and year of birth. Credit header data is obtained from consumer reporting agencies.[1] The compilation of credit header data is subject to the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801 *et seq.*, and information subject to the GLBA cannot be distributed except for purposes specified by the Congress, such as the prevention of fraud.

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

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

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

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

Other laws:

Unfair and Deceptive Practice Laws: Section 5 of the Federal Trade Commission Act, and its state counterparts, prohibit companies from making deceptive claims about their privacy and security practices. These laws have served as the basis for enforcement actions by the Federal Trade Commission and state attorneys general for inadequate information security practices. The consent orders settling these enforcement actions typically have required

companies to implement information security programs that conform to the standards set forth in the GLBA Safeguards Rule, 16 C.F.R. Part 314.

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

Legislative Measures LexisNexis Supports

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

Data Security Breach Notification. We support requiring notification in the event of a security breach where there is substantial risk of harm to consumers. It is important that there is an appropriate threshold for when individuals actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that it is important that any such legislation contain federal preemption to insure that companies can quickly and effectively notify individuals and not struggle with complying with multiple, potentially conflicting and inconsistent state laws.

Adoption of Data Security Safeguards for Information Service Providers Modeled After the GLBA Safeguards Rule. LexisNexis supports the adoption of data security protections for information service providers modeled after the Safeguards Rule of the GLBA.

Increased penalties for identity theft and other cybercrimes and increased resources for law enforcement. LexisNexis strongly encourages legislation that imposes more stringent penalties for identity theft and other cybercrimes. Additionally, consumers and industry alike would benefit from enhanced training for law enforcement and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and cybercrime. Too many of our law enforcement agencies do not have the resources to neutralize these high-tech criminals.

Finally, LexisNexis strongly encourages that any legislation considered strike a balance between protecting privacy and providing legitimate businesses, organizations, and government agencies with access to critical information that enables them to fulfill their important missions.

I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the protection of consumer information. I look forward to working with the members of this committee as you consider these important public policy issues.

TESTIMONY OF BESTOR WARD

Member of the

NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION, INC. ("NAID")

Before the

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

Hearing on

ASSESSING DATA SECURITY:

PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION

MAY 4, 2005

I. Introduction

Mr. Chairman and members of the Committee, I am Bestor Ward, a member of the National Association for Information Destruction, Inc. ("NAID"). I appreciate the opportunity to appear before you today to discuss the important role that proper information destruction plays in the fight against identity theft. NAID commends the Committee for addressing this critical issue.

I am President of Safe Archives – Safe Shredding, a business that provides secure records management, media storage, and information destruction services in Mobile, Alabama and the surrounding area. I am a member of NAID's Governmental Relations Committee. I also serve on the boards of the J.L. Bedsole Foundation and AmSouth Bank N.A. Through these professional roles, I have gained first-hand experience about identity theft. As an AmSouth Bank director, I receive regular updates on the incidence of identity theft affecting the bank. The J.L. Bedsole Foundation has been the victim of identity theft; on two separate occasions the foundation's credit card was used by an identity thief who made expensive charges on the card. As President of Safe Archives – Safe Shredding, I run a business dedicated to storing and destroying confidential records securely, so that they do not fall into the wrong hands.

NAID is the international, non-profit trade association of the information destruction industry. NAID and its individual members are expert in, and committed to, the proper destruction of paper records and other media containing sensitive financial or personal information that could be misused by identity thieves. NAID's mission is to champion the responsible destruction of confidential information and materials by promoting the highest standards and ethics in the industry. NAID members are bound to a strict code of ethical practices. NAID has a Complaint Resolution Council that is dedicated to reviewing ethical

complaints and recommending appropriate actions (up to and including fines and expulsion) to the NAID Board of Directors. In addition, NAID offers an annual operations certification program to its members, which establishes standards for employee hiring and screening, operations, the destruction process, and insurance, as well as other security factors.

My testimony today covers four main points. First, I will discuss the serious problem of identity theft, which is caused in part by improperly discarding sensitive consumer information. Second, I will address the current legislation that governs information privacy, including the Fair and Accurate Credit Transactions Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. Third, I will argue that, while these laws represent positive steps towards preventing unauthorized access to personal information, they leave significant gaps in coverage. Finally, I will discuss NAID's recommendations for new, uniform legislation to fill these gaps in order to prevent identity theft.

II. Improper Information Destruction and Identity Theft

As this Committee recognizes, identity theft is a serious crime that imposes enormous costs on society. Tens of millions of Americans have been victims of identity theft, costing consumers and businesses tens of billions of dollars.[1] In 2004 alone, 246,570 identity theft complaints were reported to the FTC.[2]

In addition to tangible economic losses, identity theft victims face lost job opportunities, loan denials, and huge intangible costs as they devote months and years to rectifying their

---

[1] Synovate/FTC, Identity Theft Survey Report 6-7 (Sept. 2003), *at* http://www.ftc.gov/os/2003/09/synovatereport.pdf; *see also*, Report: Overview of the Identity Theft Program (Oct. 1998 – Sept. 2003) (Sept. 2003), *at* http://www.ftc.gov/os/2003/09/timelinereport.pdf.

[2] FTC, National and State Trends in Fraud & Identity Theft (January – December 2004) 4 (February 1, 2005), *at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

damaged credit records. Identity theft also poses a serious threat to public safety. Terrorists and other criminals, for example, may open bank accounts under false names, launder money using false identities, and use fraudulently obtained drivers licenses to avoid detection. While making identity theft more difficult will not prevent the determined terrorist or criminal from assuming a false identity, the protection of sensitive information can make it more difficult for them to do so. Numerous identity theft crimes are committed by so-called "dumpster divers" who uncover and misuse sensitive paper and electronic documents after they have been discarded. Many hearings to date have focused on controlling or limiting the sale or transfer of personal information. Yet, such controls are undermined when the ultimate disposal of sensitive consumer information is not regulated. It simply does not make sense to implement information-transfer controls while ignoring the fact that this same information is often being placed in the trash for anyone to take.

Identity theft is a crime of opportunity, and it is vital that we take steps to reduce criminal opportunities. One of the most efficient and effective ways to fight identity theft is to prevent it by ensuring secure records management and proper disposal of confidential information at the point when documents are discarded in the normal course of business. It makes far greater sense to enact strong laws that prevent so-called "dumpster divers" and other criminals from accessing information, than waiting until after massive losses have occurred and attempting (often unsuccessfully) to find and prosecute the perpetrators after the fact. Relying on after-the-fact prosecution to fight identity theft is particularly ineffective, considering that approximately 61% of victims who reported identity theft to the FTC in 2004 did not notify any police department.[3]

---

[3] FTC, National and State Trends in Fraud & Identity Theft (January – December 2004) 11 (February 1, 2005), *at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

III. Current Legislation Governing Information Privacy and Identity Theft

NAID commends Congress for combating identity theft by enacting the Fair and Accurate Credit Transactions Act ("FACT Act"), the Gramm-Leach-Bliley Act ("GLBA"), and the Health Insurance Portability and Accountability Act ("HIPAA"). However, NAID recognizes that the existing federal and state consumer fraud legislation leaves significant gaps in coverage. NAID thanks this Committee for its attention to this serious matter, and encourages the Committee to take further steps to fill these gaps. In particular, NAID supports strong, uniform information disposal legislation that broadly covers all businesses that possess documents containing consumer information subject to misuse.

A. The FACT Act and Disposal Rules

Pursuant to the FACT Act, the Federal Trade Commission ("FTC") has adopted a rule entitled, "Disposal of Consumer Report Information and Records"[4] ("FTC Disposal Rule"), which will take effect on June 1, 2005.[5] Under that rule, businesses are required to properly dispose of and to destroy "consumer information," which is defined as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records."[6] In turn, the FACT Act defines "consumer report" as any "communication of any information by a

---

[4] 16 C.F.R. Part 682.

[5] The Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Comptroller of the Currency, the Federal Reserve System, the Office of Thrift Supervision, and the National Credit Union Administration also promulgated rules pursuant to the FACT Act. 69 FR 71322 to be codified at 17 C.F.R. Part 248; 69 FR 77610 to be codified at 12 C.F.R. Parts 334, 364; 69 FR 77610 to be codified at 12 C.F.R. Parts 30, 41; 69 FR 77610 to be codified at 12 C.F.R. Parts 208, 211, 222, 225; 69 FR 77610 to be codified at 12 C.F.R. Parts 568, 570, 571; 69 FR 69269 to be codified at 12 C.F.R. Parts 717, 748.

[6] 16 C.F.R. § 682.1(b).

consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living," which is intended to assist in "establishing the consumer's eligibility for — (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes;" or other authorized purposes.[7]

The FTC Disposal Rule specifically requires any person or company that possesses or maintains "consumer report" information to "tak[e] reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[8] The rule provides examples of how to comply with this standard, including:

- Implementing and monitoring compliance with policies and procedures that require shredding or other forms of destruction of documents and electronic media containing consumer information; and
- Contracting with a third party to properly dispose of consumer information and monitoring their performance.

By June 1, 2005, entities over which the FTC has authority[9] must adopt and implement their own document destruction policies or contract with a document shredding company or other data destruction company to do so. Penalties for violating the rule include actual damages;

---

[7] 15 U.S.C. § 1681a(d)(1). This definition is also subject to some exclusions. 15 U.S.C. § 1681a(d)(2).

[8] 16 C.F.R. § 682.3(a).

[9] The FTC has authority to enforce compliance under the Federal Trade Commission Act. The FTC's jurisdiction extends over entities except certain banks, savings and loan institutions, federal credit unions, common carriers, air carriers, insurance companies, and others subject to the Packers and Stockyards Act. 15 U.S.C. §§ 1681s, 1681w; 15 U.S.C. § 1012.

statutory damages up to $1,000; punitive damages; attorneys' fees; and civil penalties up to $2,500 per violation.

Although the FTC's Disposal Rule holds great promise in combating identity theft, its effectiveness is limited by the fact that it reaches only "consumer report" information. In the end, however, individuals could just as easily become victims of identity theft through compromise of their personal information from sources other than consumer reports, such as discarded credit card records or computer tapes placed in the trash. Enormous cost, inconvenience, and a sense of violation can be avoided through the simple expedient: proper disposal of all documents containing sensitive consumer information.

B. The Gramm-Leach-Bliley Act and FTC Safeguards Rules

The FTC's Disposal Rule supplements the privacy provisions set forth in the Gramm-Leach-Bliley Act, and its associated agency rules. The Gramm-Leach-Bliley Act governs financial institutions, and protects the privacy of non-public consumer information. The FTC promulgated "Standards for Safeguarding Customer Information" ("FTC Safeguards Rule") pursuant to the Gramm-Leach-Bliley Act. Under the FTC Safeguard Rule, covered entities are required to, "develop, implement, and maintain a comprehensive information security program" that contains appropriate "administrative, technical, and physical safeguards."[10] Such safeguards must be reasonably designed to: "(1) Insure the security and confidentiality of customer information; (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[11]

---

[10] 16 C.F.R. § 314.3(a).

[11] 16 C.F.R. § 314.3(b).

Notably, if a financial institution decides to retain a third party to safeguard its customer information, the FTC Safeguards Rule requires that it "[o]versee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring [] service providers by contract to implement and maintain such safeguards."[12] Accordingly, a financial institution must either take internal steps to safeguard customer information or contract with a "capable" third party to do so.

The major limitation of the FTC Safeguards Rule is that it applies only to financial institutions. NAID agrees with the position of FTC Chairman Deborah Platt Majoras that Congress should extend this rule to apply more broadly, beyond financial institutions.[13] There is no reason to limit these requirements to financial institutions. Rather, all record owners should be required properly to dispose of sensitive customer information or, after conducting due diligence, to contract with a capable record disposal company to do so and to monitor the disposal company's performance.

NAID supports various due diligence efforts, including record owners reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal

---

[12] 16 C.F.R. § 314.4(d). Similarly, under the U.S. Department of Health and Human Services standards for HIPAA, a covered entity that permits a business associate to maintain its electronic protected health information must enter a written contract or other written arrangement that documents satisfactory assurances that the business associate will appropriately safeguard the information. 45 C.F.R. § 164.308(b)(1), (4). In particular, such a contract must provide that the business associate will "[i]mplement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information" in its possession. 45 C.F.R. § 164.314(a)(2)(i)(A).

[13] "Congress Likely to Pass Firm Legislation Targeting Identity Theft, Sen. Specter Says," 84 BNA Banking Report 712 (April 18, 2005).

company. Another worthwhile due diligence effort suggested by the FTC involves the certification of disposal companies by a recognized trade association.[14]

C. HIPAA

HIPAA governs the use and disclosure of individually identifiable health information.[15] Under the U.S. Department of Health and Human Services standards, health plans, health care clearinghouses, and certain health care providers are required to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[16] Accordingly, HIPAA adds an important information security mandate by requiring covered businesses to take precautions to protect the privacy of patient information that could be used to commit identity theft. However, as with FCRA and GLBA, HIPAA's reach is limited, leaving many documents with sensitive personal information unprotected.

IV. The Need for Additional Legislation

While the FACT Act, the GLBA, and HIPAA represent important steps towards preventing identity theft, they are too limited in scope. Specifically, the FACT Act and its associated rules only cover "consumer report" information. Many other documents contain information that can be used to facilitate identity theft. It makes little sense to impose strict requirements on the disposal of "consumer report" information, but not other, equally sensitive personal information derived from other sources. Requirements under Gramm-Leach-Bliley and HIPAA, and their associated rules, are also too limited in scope because they apply only to financial institutions and health care businesses, respectively. Accordingly, despite the recent

---

[14] 16 C.F.R. § 682.3(b)(3).

[15] 42 U.S.C. § 1320d-6.

[16] 45 C.F.R. §§ 160.103(3), 164.308.

legislative and regulatory steps taken to fight identity theft, the resulting patchwork of legal authority leaves significant gaps in coverage.

NAID proposes that Congress consider expanding on the current legal requirements by addressing the complete set of businesses and information affected by identity theft. NAID specifically sets forth three proposals for such broad-based legislation.

First, global anti-identity theft legislation should apply more broadly to all records that contain sensitive consumer information, including credit card and bank information, Social Security Numbers, telephone numbers, and addresses maintained by anyone in business.

Second, written privacy policy disclosures provided to consumers should include a statement that details the company's responsibility to destroy all discarded personal information. Consumers should also be made aware that they can request a full disclosure on how any company accepting personal information destroys it when it is discarded.

Third, senior company officers should be responsible for implementing and overseeing their business' disposal policies. Good models for this approach can be found in the Sarbanes-Oxley Act, and in the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which were promulgated by the Federal Deposit Insurance Corporation ("FDIC"), the Comptroller of the Currency, the Federal Reserve System, the Office of Thrift Supervision, and the National Credit Union Administration pursuant to Gramm-Leach-Bliley ("GLBA Safeguards Rules"). The GLBA Safeguards Rules assign responsibilities to "[t]he board of directors or an appropriate committee of the board."[17] Specifically, these individuals shall:

[17] 12 C.F.R. § 30, App. B § III(A); 12 C.F.R. § 225, App. F § III(A); 12 C.F.R. § 364, App. B § III(A); 12 C.F.R. § 570, App. B § III(A); 12 C.F.R. § 748, App. A § III(A). The FDIC, the Comptroller of the Currency, and the Federal Reserve System define board of directors as the

"(1) Approve the [entity's] written information security program; and (2) Oversee the development, implementation, and maintenance of the [entity's] information security program, including assigning specific responsibility for its implementation and reviewing reports from management." NAID recommends that Congress apply these models for corporate responsibility by requiring appropriate senior officials to implement and supervise disposal policies that meet the requisite legal standards. Compared to the high costs that victims and the law enforcement community incur after identity theft has been committed, it is far more efficient to require proper methods of disposal to prevent the misuse of sensitive consumer information.

V. Conclusion

I will close with an anecdote. Shortly after Georgia enacted information destruction legislation in May 2003, NAID received a call from an employee of a well-known national corporation. The caller asked for a list of Georgia companies that it could retain to shred documents covered by the state's new disposal requirements. The caller was located in the company's corporate headquarters outside of Georgia, and our NAID representative offered to send a broader list of NAID member-companies that operate in other states where the company conducts business. The caller's response was, "No thanks, the other states don't have shredding laws." This response highlights the need for strong, uniform federal legislation that closes the gaps between existing laws by requiring all businesses to properly dispose of sensitive financial and personal information that is subject to misuse.

"managing official in charge of the branch or agency." 12 C.F.R. § 30, App. B § I(C)(2)(a); 12 C.F.R. § 225, App. F § I(C)(2)(a); 12 C.F.R. § 364, App. B § I(C)(2)(a).

Mr. Chairman, we commend the Committee's interest in strengthening protections against identity theft. Thank you for inviting me to discuss this topic. I look forward to answering your questions.

Biography: Bestor Ward

Bestor Ward, president of Ward Properties, Inc., graduated from Auburn University in 1980 with a degree in marketing. Ward worked for a local bank before entering into the commercial real estate industry working for White-Spunner Commercial Development. In 1989 he joined the family-owned business, Bedsole Investment Company, Inc. which has been in continuous business in Mobile since 1928. Later he acquired the majority of the company stock and changed the name to Ward Properties, Inc. Safe Archives – Safe Shredding is a wholly owned subsidiary of Ward Properties, Inc. Ward and the Safe Archives - Safe Shredding team have become the leader in secure, quality service for records management, media storage and information destruction in the Greater Mobile Metropolitan area.

Since forming Safe Archives – Safe Shredding, Ward has become passionate about the records management industry and has become a champion of the business by educating himself and his team about business safety and security on records management issues. After receiving the counsel of numerous top industry consultants and attending industry training, Ward has become a subject-matter expert. Recently, the National Association of Information Destruction (NAID), the group known for setting the standards for the information destruction, appointed Ward to their national Governmental Affairs Committee.

Ward has extensive Civic and Business affiliations throughout Mobile and the State of Alabama and he has served on the board of many organizations including The Mobile Area Chamber of Commerce, The Rotary Club of Mobile and The J.L. Bedsole Foundation and AmSouth Bank N.A.

Safe Archives- Safe Shredding parent company, Ward Properties, Inc., has been doing business along the northern Gulf Coast since 1928 and has an extensive history of community involvement and support.

Updated 04/21/2005

RON PAUL
14TH DISTRICT, TEXAS

FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEES:
VICE CHAIRMAN
OVERSIGHT AND INVESTIGATIONS
DOMESTIC AND INTERNATIONAL
MONETARY POLICY, TRADE AND TECHNOLOGY

INTERNATIONAL RELATIONS COMMITTEE
SUBCOMMITTEES:
ASIA AND THE PACIFIC
WESTERN HEMISPHERE

JOINT ECONOMIC COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–4314

203 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2831

312 SOUTH MAIN
SUITE 228
VICTORIA, TX 77901
(361) 576-1231

200 WEST 2ND STREET
SUITE 210
FREEPORT, TX 77541
(979) 230-0000

May 25, 2005

The Honorable Michael Oxley
Chairman
Committee on Financial Services
2129 Rayburn HOB
Washington, DC 20515

Dear Honorable Oxley:

Thank you for holding the hearing on "Assessing Data Security: Preventing Breaches and Protecting Sensitive Information." Unfortunately, a scheduling conflict prevented me from attending. I would greatly appreciate it if the committee would insert the following statement from my constituent Mr. Kenneth Don Schustereit from Victoria, Texas, into the official hearing record. Mr. Schustereit's statement details the problems he is experiencing because ChoicePoint, Inc.'s database mistakenly identifies his 30-year old misdemeanor conviction as a felony conviction. Mr. Schustereit believes that ChoicePoint, and the Texas Department of Public Safety that was the original source of the mistaken information, demonstrated gross negligence in this case. Mr. Schustereit also believes that neither has made adequate efforts to correct its records or compensate him for the damage caused by disseminating the inaccurate information. I have also attached two stories from Wired magazine dealing with Mr. Schustereit's situation.

I would also appreciate it if the committee would add Mr. Schustereit to the list of prospective witnesses for future hearings on this matter. I, and my staff, have had the privilege of knowing Mr. Schustereit for a number of years since he is very active in his community. I am therefore pleased to recommend that the Committee on Financial Services invite Mr. Schustereit to testify at a further hearing dealing with the issues surrounding the misuse of individuals' personal data by companies such as ChoicePoint.

Please contact Mr. Norman Singleton, my legislative director, if you need any more information from my office regarding Mr. Schustereit's case. Thank you for your attention to my constituent's concerns.

Sincerely,

Ron Paul

Ron Paul

Enclosures

cc: Rep. Barney Frank, Ranking Member

My name is Kenneth Don Schustereit from Victoria, Texas. I am proud to call Congressman Paul my Congressman.
I contact you today in an effort to convince you to hear my testimony on the conduct of ChoicePoint, Inc. whose Chairman and CEO has also recently given testimony before your committee.
When I was 18 years old I made a silly mistake and got in trouble with the law. I picked up some, of what I took for scrap iron, from an open parking lot. I got caught and the owner was called. He valued it at $2700 and I was charged with a felony. This was later reduced to a misdemeanor and I was sentenced to 60 days in the County Lockup. I subsequently was made a trustee and released after 51 days. No deferred adjudication, no community service, no fines and no probation. I served that time between my Junior and Senior years of High School.
Fast forward to November of '01 and all of the sudden I was finding it next to impossible to go to work. There was plenty of work but I couldn't get hired anywhere. Finally, after 10 months I took a job making much less money and was happy to get it.
After that job played out I wrote a new resume and began looking around late last summer I applied for a part time position at Lowe's in the electrical department selling light bulbs and wire nuts. I was told that my criminal background was keeping me out. I didn't understand it. I admitted to having a misdemeanor 30 years ago. What was the deal? No explanation! They just wouldn't hire me. I had a good work record and 7 letters of recommendation. Still no hire!
I decided to go around the corner to Home Depot. I did a computer application. Admitted that I had a 30 year old misdemeanor and even spoke with the Human Resources person, Kathy Schumaker. She said don't worry. She asked if it was drugs and I told her it wasn't and that it was 30 years ago. She smiled and said that's no problem, they only go back a few years and were concerned about drugs primarily.
I spoke with the store manager and we agreed on a wage and went for and passed the drug test. Then about a week later I got a letter from

Home Depot that said they were considering a negative impact on my employment application because of a criminal background check. I must say my heart sank. Christmas was coming up and I needed to work. ChoicePoint indicated that I was a convicted felon and implied that I had served seven years. I called their 800 number and found that it could take up to 30 days to clear this up. Meanwhile I went to the District Clerk's office and got a copy of the cause against me and mailed it to both ChoicePoint and the Texas Department of Public Safety.

It should have been obvious to ChoicePoint that something was wrong because they had my name wrong. All someone had to do was check the Court Record.

I also found out that the Texas DPS never said I served seven years for anything. Since ChoicePoint bought the record fro the DPS I can only conclude that they embellished on it.

Meanwhile Home Depot has filled my job with someone else and I'm hanging in the wind while Derek Smith is liquidating his stock.

Did ChoicePoint notify me they were giving selling an adverse background check on me? No! Did ChoicePoint follow any procedure to make sure the information they got from DPS was correct? No! Is ChoicePoint aware that up to 60% of DPS records are out of date or incorrect? Of course! The whole industry know of it! Did ChoicePoint violate the Fair Credit Reporting Act? Yes they did! Has my business reputation been slandered and libeled by a willful act of negligence and irresponsibility on the part of ChoicePoint? Yes!

I seek the opportunity to address congress on this matter since there were literally thousands of others who have suffered because of ChoicePoints irresponsible and reckless method of operating their business. I ask whether it is reasonable for a man to face his accuser before Congress?

Kenneth Don Schustereit
361-5705994 5784436

ChoicePoint's Checks Under Fire

By Kim Zetter

Story location: http://www.wired.com/news/privacy/0,1848,66983,00.html

02:00 AM Mar. 23, 2005 PT

As data broker ChoicePoint wrestles with the fallout from the sale of personal data to identity thieves and an investigation into two executives' sale of company stock, it faces questions on another front: its background-checking services.

Several lawsuits and consumer complaints in the last few years have accused ChoicePoint of providing inaccurate and out-of-date information in its criminal background reports, resulting in unfair job losses for applicants.

Even though a federal law requires consumer reporting agencies -- as third parties who conduct background checks for employers are called -- to either verify the data they give employers or notify job applicants when they provide adverse information to an employer, ChoicePoint appears to be doing neither in some cases.

The company was found guilty of breaking the law in one case in which an applicant lost a job over outdated information, but other cases were settled out of court or are still being investigated.

Under Section 613 of the Fair Credit Reporting Act, or FCRA, consumer reporting agencies that use public records -- such as criminal arrest and conviction records -- to conduct background checks must "maintain strict procedures" to ensure that information they give employers matches the most current public records if the information might adversely affect a job applicant.

But many reporting agencies, particularly ones that offer instant online background checks, collect data in bulk from state and local databases and store it for subsequent background searches, updating the data only once every seven, 30, 60 or even 90 days.

Mike Coffey, president of a Texas investigation firm, contends that even periodically refreshing data from state and local databases isn't sufficient to obtain current data, since courts update records daily and state repositories

can't keep pace with every court. A felony charge one day could be reduced to a misdemeanor the next day, and unless investigators examined courthouse records when they conducted a background check, they couldn't be sure they were giving employers the most current data.

"We always go back to the source and verify it," said Coffey, who teaches background investigation courses for law enforcement, private investigators and corporate security departments. "That's the only responsible thing to do so that you don't cost somebody a job."

The law provides a loophole for reporting agencies, however, by allowing them not to provide up-to-date data if, when they give an employer a background report containing adverse information, they also tell the applicant about the report and give the applicant the name and address of the employer who received it. This is designed to prevent employers from conducting background checks without an applicant's permission, which the law requires them to obtain.

But Coffey said many reporting agencies don't adhere to this requirement either.

"There's a group of us who want to do this right," Coffey said. "And then there are a number of companies just out to make a quick buck who don't have any concern about the quality of what they're doing."

Ken Schustereit, who was featured in a previous story about background checks, said ChoicePoint never notified him when it reported, erroneously, to Home Depot that he was a convicted felon who had served seven years in prison.

Schustereit learned about the report only when Home Depot rejected him for the job -- federal law requires companies to tell applicants when a background check is the cause for a job loss.

Another applicant who recently lost a job with a management consulting firm also said ChoicePoint never contacted him when it reported a felony theft arrest that the courts had expunged from his record. The applicant, who asked to remain anonymous since he's still looking for a job, was arrested in 2000, but received a year's probation. His record was expunged in 2001.

ChoicePoint provided a clean background check when he applied for his first job out of college in 2003, but a report provided for a new employer in 2005 showed the arrest.

ChoicePoint removed the arrest after the applicant complained, but the

consulting company rescinded its job offer anyway, saying his background could turn off clients if they knew.

In New York in 2001, Abel Obabueki sued ChoicePoint for similar reasons after IBM rescinded a job offer when ChoicePoint in 1999 indicated he'd been convicted of welfare fraud. The misdemeanor conviction had been dismissed in 1997, and the case was expunged.

Greg Antollino, Obabueki's attorney, said ChoicePoint never sent his client a letter telling him it was providing adverse information to IBM as the law required. ChoicePoint sent a revised report after Obabueki complained, "but the damage had already been done," Antollino said.

The court concluded that ChoicePoint had broken the law, but an appeals court concluded that the company owed Obabueki no damages because Obabueki couldn't prove IBM's decision was due to the background report.

Tom Wilder, district clerk for Tarrant County, Texas, says expunged records are one reason he refuses to sell his county's public records to database companies in bulk

"Even if they update weekly, their information is going to be out-of-date and a background check may not reflect what happened in the case," Wilder said. "It's not fair to the individual who has a right to get something off their record."

Wired News asked ChoicePoint if the company notified applicants when providing employers with adverse information about them. Spokesman Chuck Jones initially said ChoicePoint wasn't required to do so because applicants knew a background check was occurring when they gave an employer permission to conduct it.

But when told the law does require it if ChoicePoint doesn't provide up-to-date information, he said he'd have to investigate and call back. He later said that ChoicePoint did notify applicants, although he couldn't "speak to the specific circumstances" around people who said they weren't notified.

Jones said ChoicePoint also followed the FCRA's alternative requirement, refreshing its data "as often as the government entity that houses the data refreshes" -- which could be weekly, monthly or quarterly -- and keeping it "as accurate and up-to-date as it could be."

But according to the Texas Department of Public Safety, from whom ChoicePoint received its data about Schustereit, ChoicePoint did not keep current with its records.

Tena Mange, spokeswoman for the department, which serves as a repository for public records from around the state, said the department refreshed its data daily -- hourly in the case of sex offenders -- but ChoicePoint bought the data only once a month.

"It gets kind of expensive," Mange said. "They may have decided that's the rate at which they feel confident in doing it."

Coffey said that unless ChoicePoint physically visited county courthouses to obtain data, it couldn't claim to have current information because the Texas DPS was notorious for having incomplete, out-of-date and missing criminal records.

A report by the Texas DPS in July revealed that the state database had only 69 percent of all criminal records available for the state in 2002 and only 60 percent for 2001. In October the *Dallas Morning News* found that more than 4,000 Dallas County records involving sex offenders were not in the state database, either.

Texas counties are required to submit their public records to the state, but there's no penalty for failing to do so. As a result of huge gaps in the state database, Mange said her department regularly tells people to go to the local courts if they want the most up-to-date information.

Jones said his company obtains thousands of public records daily -- sometimes through electronic means and sometimes through contract workers who visit courthouses.

He didn't say when they conducted courthouse visits but they likely didn't occur for customers who purchased instant online background reports through the company's ScreenNow service, or through Rapsheets Criminal Records, a Tennessee company ChoicePoint purchased last year. Rapsheets is specific about what it does and doesn't do for customers. Its website says it delivers low-cost, instant searches of archived records as "an alternative to more expensive and time-consuming in-person, courthouse searches."

The company also offers a mixed message about the thorough and accurate nature of its data. Although it claims to offer "the most complete and up-to-date information available on the internet," it admits that its service "does not always substitute for an in-person courthouse search of criminal records."

Although the Federal Trade Commission is supposed to enforce statutes governing consumer reporting agencies, it doesn't monitor companies unless it receives specific complaints about a pattern of illegal behavior. FTC

lawyer Clark Brinkerhoff told Wired News that he'd never even had to research the statute related to background checks, because complaints related to it had never come up.

According to a letter that an FTC lawyer wrote in 1999 to a Dallas investigating firm, a reporting agency that uses stored data for background checks is clearly breaking the law if it doesn't immediately update its data from public records before it reports the information to employers or notify applicants when it provides the public record information report to employers.

The letter was unclear, however, which public records a company should check -- those in a state repository or those in a county courthouse.

But Brinckerhoff told Wired News that because the law requires reporting agencies to maintain "strict procedures" to ensure data is up-to-date rather than merely "reasonable procedures," it's clear the agencies are required to take extra steps to get the freshest data.

"If the options are taking someone else's word for (the accuracy of the data) or going to the courthouse, I'd argue that you've got to do the latter," Brinckerhoff said.

Brinckerhoff also said that if ChoicePoint obtained data from a source that was known to have incomplete and incorrect data, it could be held liable for lack of due diligence under the FCRA.

"If it's true that the Texas DPS has lousy data and it's commonly known and I can prove that in a court of law, I can win a case against someone for not having strict procedures," Brinckerhoff said.

The problem is that ChoicePoint and other consumer reporting agencies could simply avoid the requirement to provide current and accurate data if they notified applicants when they gave employers negative background reports, which means they could legally sell out-of-date and erroneous information -- even though it could harm job applicants as well as employers -- and take no responsibility for the consequences.

"Unfortunately, this is an industry that has an allergic reaction to admitting any fault," said Chris Hoofnagle, director of the West Coast office for the Electronic Privacy Information Center. "They're infallible in their own eyes. And no one's doing anything to make them take responsibility."

Bad Data Fouls Background Checks

By Kim Zetter

Story location: http://www.wired.com/news/privacy/0,1848,66856,00.html

02:00 AM Mar. 11, 2005 PT

When Kenneth Schustereit was 18 years old, he tried to swipe a pile of what he thought was scrap metal from a machine shop's parking lot and ended up spending part of his summer vacation in jail for misdemeanor theft.

That was in 1974. Thirty years later, Schustereit is still paying for his crime.

That's because a background check of his criminal record sold to employers by ChoicePoint data brokers erroneously reported that his misdemeanor was a felony. It also stated that he spent seven years in prison when he spent 51 days in county jail.

Schustereit discovered the mistake only after Home Depot turned him down for a job last year and mentioned the report. He thinks the report cost him half a dozen other jobs as well, although he doesn't know for sure, since most employers don't tell job applicants why they've been rejected.

"I have a stellar work record," said Schustereit, who was laid off nine months ago as a quality-assurance inspector at a Texas plant. "But the problem is that I write down a 30-year-old misdemeanor on the application, and when they look it up, it comes up as a felony. It makes me look like a lying convict."

Recent security breaches at ChoicePoint and Seisint have raised awareness about data brokering and the role that these companies play in identity theft.

But the breaches have brought little attention to another problem with data brokering that can cause just as much harm as identity theft -- inaccurate data.

In addition to selling personal information about millions of people to marketers and government agencies, data brokers collect information from public records and sell it to employers conducting background checks on prospective workers.

Employers facing problems with violent workers, falsified credentials and workplace theft have legitimate reasons for seeking background checks. And obtaining such reports has become increasingly easy and cheap when masses of information can be collected electronically and sold online.

But there are no standards for assuring the accuracy of data. And incorrect or misleading information can lead to lost jobs and public embarrassment.

Legislation is currently going through Congress that would establish oversight of data brokers to help prevent identity theft, but it doesn't address problems with data accuracy. The onus for finding errors and correcting them will still be on members of the public.

A 2004 report by the National Association of State Public Interest Research Groups found that 79 percent of credit reports may contain some type of error. There's no reason to believe that criminal records are any more accurate.

The Fair Credit Reporting Act, which covers background checks for issues related to employment, requires that employers get written permission from subjects to perform a check on them. But workers seldom have a choice in the matter if they want a job. If applicants or employees lose a job or promotion because of information in a background check, workers are entitled to receive a copy of the report from the data broker that provided it.

"But what's to prevent a company from doing a check and saying they're not going to hire you for another reason?" said Ronald Peterson, who believes he lost jobs because of his reports. "You and I don't have a right to look at who has asked for our records."

Getting misinformation in a file corrected or removed is another battle.

Misinformation can occur for a number of reasons -- clerks mis-key information, criminal charges get dropped but not updated in files, or arrested suspects provide authorities with the name and Social Security number of someone else. If data does get corrected in one database, there is no way to ensure that it's corrected in other databases.

Easy access to masses of digital data that never goes away also means that people are less able to make a clean start in life even after they've served their time or been cleared of charges.

After the terror attacks of Sept. 11, 2001, pharmaceutical company Eli Lilly ran criminal background checks on more than 7,000 employees working for its outside vendors and barred hundreds of workers from the company,

including a man who lost his position because of a 6-1/2-year-old dismissed misdemeanor battery charge that should have been expunged from his record.

"We're becoming a nation where there is no social forgiveness," said Beth Givens, founder and director of the Privacy Rights Clearinghouse. "We've got to have wiggle room in our society to accept mistakes we've made in the past. But you can't do that anymore because of records being permanently in these databases."

Schustereit is a case in point.

After being laid off from his job, he applied for work in Home Depot's electrical department. He'd passed a drug test and psychological review and had even discussed salary and working hours with the company. But then Home Depot told him his background didn't check out.

It took several calls to ChoicePoint and Home Depot's headquarters before Schustereit discovered that ChoicePoint had listed him as a felon. The company's report also listed his middle name as Dale instead of Don, which suggested that the company might have confused him with someone else.

Ron Peterson's problem was even more pronounced than Schustereit's. A report from backgroundchecks.com attributed him with an array of serious criminal offenses he never committed.

"In Florida I'm a female prostitute (named Ronnie); in Texas I'm currently incarcerated for manslaughter," Peterson, a California resident, said. "In New Mexico I'm a dealer of stolen goods. Oregon has me as a witness tamperer. And in Nevada -- this is my favorite -- I'm a registered sex offender."

Back in 1974, Schustereit was originally charged with third-degree felony theft. But in a deal with authorities, he pleaded guilty to a misdemeanor instead and was sentenced to 60 days in jail. He was released early for good behavior. But the ChoicePoint report failed to note either of these significant details.

ChoicePoint blamed the Texas Department of Public Safety, where it said the incorrect felony information originated. The Texas DPS did admit to misidentifying Schustereit's offense, but not for turning his 60-day sentence into seven years. The department said ChoicePoint was responsible for that error.

Schustereit thinks the mistake is indicative of the sloppy work that data

brokers do.

"It was incumbent on both the Texas DPS and ChoicePoint to find out if Kenneth Dale was different from Kenneth Don before ruining someone's life," he said.

Texas DPS spokeswoman Tena Mange said her department has quality-control procedures for information that it creates but has little control over the accuracy of electronic data that comes from courts and arresting authorities. And after information leaves the DPS office, the department has no control over how data brokers manipulate it.

Mange said her department always recommends that people counting on criminal background checks for hiring decisions conduct fingerprint matches instead of name matches, even though they're more expensive and take more time.

ChoicePoint declined to comment for this story and Home Depot did not return calls for comment.

After numerous phone calls and e-mails, ChoicePoint and the Texas DPS did fix Schustereit's record, although the damage was already done. And Schustereit has no idea how many other data brokers still list him as a felon.

Peterson had to work hard to get his record cleaned up. He bought reports from ChoicePoint and backgroundchecks.com after State Farm denied him insurance last year. ChoicePoint got his middle name wrong and reported that there was a bench warrant for his arrest in Arizona.

Backgroundchecks.com -- which claims to have 4,000 customers worldwide, including Fortune 500 companies -- included information about all Ronald or Ronnie Petersons in its database, apparently making no attempt to distinguish relevant records from irrelevant ones, even when Peterson inserted different birth dates to see if the information would change. It didn't.

Backgroundchecks.com President Craig Kessler said there was little data brokers could do to distinguish the records of individuals sharing the same name.

"We're not in the business of authenticating the identity of individuals. All we do is report the data that's supplied to us from the courts," said Kessler. He said the problem stems from the fact that courts are doing away with using Social Security numbers that could help distinguish people with similar names.

"Sex-offender registries do not have anything other than a name in many cases," Kessler said. "We encourage companies to ask additional questions to help them confirm that this is the same person."

But Peterson, who believes that background reports contributed to his inability to get a good job offer for the last two years, said it's easier for employers to pass on candidates who have bad information associated with their name than to do the work to determine if the information is correct.

It took Peterson 40 hours and numerous phone calls to clear his identity in Arizona -- the bench warrant was for a different Ron Peterson -- and he was able to do so only after submitting his fingerprints.

"The victim is victimized by the system," Peterson said.